Y4 J 89/1 : 103/49

MISUSE OF NATIONAL CRIME INFORMATION CENTER RECORDS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
CIVIL AND CONSTITUTIONAL RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY

AND THE

SUBCOMMITTEE ON INFORMATION, JUSTICE, TRANSPORTATION, AND AGRICULTURE

OF THE

COMMITTEE ON
GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRD CONGRESS

FIRST SESSION

JULY 28, 1993

Committee on the Judiciary
Serial No. 49

GOV'T. DEPOSITORY
JAN - 9 1
HAMPDEN LAW LIBRARY
KF 9751 .M58 1994
BOSTON PUBLIC LIBRARY GOVERNMENT DOCUMENTS DEPARTMENT

Printed for the use of the Committee on the Judiciary
and the Committee on Government Operations

U.S. GOVERNMENT PRINTING OFFICE
79-343 CC WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-046181-2

Y4.J 89/1:103/149

MISUSE OF NATIONAL CRIME INFORMATION CENTER RECORDS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
CIVIL AND CONSTITUTIONAL RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY

AND THE

SUBCOMMITTEE ON INFORMATION, JUSTICE, TRANSPORTATION, AND AGRICULTURE

OF THE

COMMITTEE ON
GOVERNMENT OPERATIONS

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRD CONGRESS

FIRST SESSION

JULY 28, 1993

Committee on the Judiciary

Serial No. 49

GOV'T. DEPOSITORY
JAN - 9 1
HAMPDEN LAW LIBRARY
KF
9751
.M58
1994
BOSTON PUBLIC LIBRARY
GOVERNMENT DOCUMENTS DEPARTMENT

Printed for the use of the Committee on the Judiciary
and the Committee on Government Operations

U.S. GOVERNMENT PRINTING OFFICE
79-343 CC WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-046181-2

COMMITTEE ON THE JUDICIARY

JACK BROOKS, Texas, *Chairman*

DON EDWARDS, California
JOHN CONYERS, JR., Michigan
ROMANO L. MAZZOLI, Kentucky
WILLIAM J. HUGHES,
MIKE SYNAR, Oklah
PATRICIA SCHROEI
DAN GLICKMAN, K
BARNEY FRANK, M
CHARLES E. SCHUI
HOWARD L. BERM/
RICK BOUCHER, Vi
JOHN BRYANT, Tex
GEORGE E. SANGM
CRAIG A. WASHINC
JACK REED, Rhode
JERROLD NADLER,
ROBERT C. SCOTT,
DAVID MANN, Ohio
MELVIN L. WATT,
XAVIER BECERRA,

HAMILTON FISH, JR., New York
CARLOS J. MOORHEAD, California
HENRY J. HYDE, Illinois

SUB

PATRICIA SCHROE
BARNEY FRANK, M
CRAIG A. WASHINC
JERROLD NADLER,

KF 9751 .M68 1994
United States. Congress.
House. Committee on the
Misuse of National Crime
Information Center records

DATE DUE

HAMPDEN LAW LIBRARY
50 State St, P.O. Box 559
Springfield, MA 01102-0559
(413) 748-7923

DEMCO

COMMITTEE ON GOVERNMENT OPERATIONS

JOHN CONYERS, JR., Michigan, *Chairman*

CARDISS COLLINS, Illinois
GLENN ENGLISH, Oklahoma
HENRY A. WAXMAN, California
MIKE SYNAR, Oklahoma
STEPHEN L. NEAL, North Carolina
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
JOHN M. SPRATT, JR., South Carolina
GARY A. CONDIT, California
COLLIN C. PETERSON, Minnesota
KAREN L. THURMAN, Florida
BOBBY L. RUSH, Illinois
CAROLYN B. MALONEY, New York
THOMAS M. BARRETT, Wisconsin
DONALD M. PAYNE, New Jersey
FLOYD H. FLAKE, New York
JAMES A. HAYES, Louisiana
CRAIG A. WASHINGTON, Texas
BARBARA-ROSE COLLINS, Michigan
CORRINE BROWN, Florida
MARJORIE MARGOLIES-MEZVINSKY, Pennsylvania
LYNN C. WOOLSEY, California
GENE GREEN, Texas
BART STUPAK, Michigan

WILLIAM F. CLINGER, JR., Pennsylvania
AL McCANDLESS, California
J. DENNIS HASTERT, Illinois
JON L. KYL, Arizona
CHRISTOPHER SHAYS, Connecticut
STEVEN SCHIFF, New Mexico
C. CHRISTOPHER COX, California
CRAIG THOMAS, Wyoming
ILEANA ROS-LEHTINEN, Florida
RONALD K. MACHTLEY, Rhode Island
DICK ZIMMER, New Jersey
WILLIAM H. ZELIFF, JR., New Hampshire
JOHN M. McHUGH, New York
STEPHEN HORN, California
DEBORAH PRYCE, Ohio
JOHN L. MICA, Florida
ROB PORTMAN, Ohio

BERNARD SANDERS, Vermont
(Independent)

JULIAN EPSTEIN, *Staff Director*
MATTHEW R. FLETCHER, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION, JUSTICE, TRANSPORTATION, AND AGRICULTURE

GARY A. CONDIT, California, *Chairman*

MAJOR R. OWENS, New York
KAREN L. THURMAN, Florida
LYNN C. WOOLSEY, California
BART STUPAK, Michigan

CRAIG THOMAS, Wyoming
ILEANA ROS-LEHTINEN, Florida
STEPHEN HORN, California

EX OFFICIO

JOHN CONYERS, JR., Michigan

WILLIAM F. CLINGER, JR., Pennsylvania

ROBERT GELLMAN, *Chief Counsel*
AURORA OGG, *Clerk*
KRISTINE I. MAMULA, *Minority Professional Staff*

CONTENTS

HEARING DATE

Page

July 28, 1993 1

OPENING STATEMENTS

Condit, Hon. Gary A., a Representative in Congress from the State of California, and chairman, Subcommittee on Information, Justice, Transportation, and Agriculture 2

Edwards, Hon. Don, a Representative in Congress from the State of California, and chairman, Subcommittee on Civil and Constitutional Rights 1

WITNESSES

Ekstrand, Laurie E., Associate Director, Administration of Justice Issues, General Government Division, U.S. General Accounting Office, accompanied by Dan Harris, Assistant Director, Law Enforcement Matters; Seto Bagdoyan, evaluator in charge; and Matthew Villarreal, evaluator 5

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Condit, Hon. Gary A., a Representative in Congress from the State of California, and chairman, Subcommittee on Information, Justice, Transportation, and Agriculture: Prepared statement 3

Ekstrand, Laurie E., Associate Director, Administration of Justice Issues, General Government Division, U.S. General Accounting Office:

Information concerning firearms purchaser screening 31

Prepared statement 7

Hyde, Hon. Henry J., a Representative in Congress from the State of Illinois: Prepared statement 35

Thomas, Hon. Craig, a Representative in Congress from the State of Wyoming: Prepared statement 4

APPENDIX

Material submitted for the hearing 39

MISUSE OF NATIONAL CRIME INFORMATION CENTER RECORDS

WEDNESDAY, JULY 28, 1993

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS, COMMITTEE ON THE JUDICIARY, AND SUBCOMMITTEE ON INFORMATION, JUSTICE, TRANSPORTATION, AND AGRICULTURE, COMMITTEE ON GOVERNMENT OPERATIONS,

Washington, DC.

The subcommittees met, pursuant to notice, at 10 a.m., in room 2237, Rayburn House Office Building, Hon. Don Edwards (chairman of the Subcommittee on Civil and Constitutional Rights) presiding.

Members present from the Subcommittee on Civil and Constitutional Rights: Representatives Don Edwards, Jerrold Nadler, Henry J. Hyde, and Howard Coble.

Members present from the Subcommittee on Information, Justice, Transportation, and Agriculture: Representatives Gary A. Condit (chairman), Lynn C. Woolsey, and Stephen Horn.

Staff present from the Subcommittee on Civil and Constitutional Rights: James X. Dempsey, assistant counsel; and Kathryn Hazeem, minority counsel.

Staff present from the Subcommittee on Information, Justice, Transportation, and Agriculture: Robert Gellman, chief counsel; Aurora Ogg, clerk; and Kristine I. Mamula, minority professional staff.

OPENING STATEMENT OF CHAIRMAN EDWARDS

Mr. EDWARDS. The two subcommittees will come to order.

This morning the Judiciary Subcommittee is holding a joint hearing with the Subcommittee on Government Information, chaired by my colleague from California, Mr. Condit.

Mr. Condit's subcommittee initially requested the GAO study that we are going to receive today, and we thank him for doing that. He and his staff have been kind enough to keep us included in this important effort. It is a matter of longstanding interest to both our subcommittees.

The hearing concerns the National Crime Information Center, known as NCIC, a computer system maintained by the FBI. The NCIC contains reports on wanted persons, missing persons, and stolen property and criminal history records. It is an extremely valuable system and we strongly support it. It is available to all State and local law enforcement agencies, really to every officer in every patrol car in the country.

The fact that the NCIC is so widely available is both the basis for its success and the source of its misuse. Everybody wants access to the NCIC.

Because we support the NCIC, we do not want to see it overloaded with inappropriate uses, and we have worked jointly with the FBI over the years to fend off requests for noncriminal justice access to NCIC. It is a criminal justice system. Because it is so widely available and is an inherently risky system, we also have worked with the FBI to limit the types of information that go into the NCIC.

Periodically, we see proposals to add to the NCIC files mere suspects, persons not wanted for arrest. The FBI in the past has rejected these proposals. One is pending right now to add suspected members of youth gangs, even if they are not wanted in connection with a crime.

As you might imagine, we are very much opposed to adding the names of people who are suspects. That has perils for our kind of society. Given the misuse of NCIC documented by the GAO, such unverified information should not go into the NCIC.

We want to address the type of abuse identified by the GAO. We are working on legislation to criminalize the misuse of the system. We hope to be able to mark this bill up early in the fall.

We look forward to the testimony of the GAO. We thank all those who worked on the report, especially Mr. Bagdoyan and Mr. Harris, who have provided valuable assistance to the subcommittee in the past.

And, of course, we are very grateful to Mr. Condit and his splendid staff.

Now I yield to the gentleman from California, Mr. Condit.

OPENING STATEMENT OF CHAIRMAN CONDIT

Mr. CONDIT. Thank you, Mr. Chairman, it is a pleasure to be here today and to join Chairman Edwards and other members of the subcommittees for this joint hearing.

Don Edwards is not only the dean of the California delegation, he is the dean of civil and constitutional rights on Capitol Hill. In that capacity, he has served as a watchdog for the National Crime Information Center for many years and it is truly a privilege to share the platform with him today.

Our two subcommittees share a common interest in the protection of the personal privacy. That is what motivated the Subcommittee on Information, Justice, Transportation, and Agriculture, which I chair, to initiate a GAO investigation of the NCIC.

In 1991, Federal prosecutors in New Jersey and Florida brought indictments against private investigators and Federal employees for illegally buying and selling confidential data from Federal Government computers, including NCIC. The indictments may only represent the tip of the iceberg.

GAO's testimony today will be important for two distinct reasons: First, it is clear that NCIC information is not adequately protected. NCIC is a vital resource for law enforcement, but its data must be protected against improper use.

Second, we can view NCIC as a model for any nationwide data base of personal information with a large number of access points.

The broader question is whether it is possible to operate such a system without opening the records to routine abuse.

These computer systems can be viewed as sort of an attractive nuisance, like a swimming pool near a school. Children are likely to use the pool and be injured, so we insist that the pool have a fence.

For a data system, the issue is whether any fence or any procedure will keep insiders from misusing data and to keep outsiders from buying access illegally. And make no mistake about it, the principal threat comes not from hackers, but from those people who have a legitimate right to access and who use that right for illicit purposes.

It appears that there are employers, insurers, lawyers or investigators who are willing to pay for illegal access to personal information, and there are some insiders who are willing to supply that data.

This is a very difficult problem, but one that we must face. The subcommittee that I chair is in the process of drafting legislation that will address the confidentiality needs of health care records. How will we be able to protect health records in a computerized environment, if we can't adequately protect criminal history records?

I hope today that we learn something about this issue and I am delighted the GAO is here today. I look forward to listening to their testimony and will submit and ask questions a little bit later, Mr. Chairman.

Thank you.

Mr. EDWARDS. Thank you, Mr. Condit. That was a really splendid statement and adds a lot to the dialog.

[The prepared statements of Mr. Condit and Mr. Thomas follow:]

PREPARED STATEMENT OF HON. GARY A. CONDIT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRMAN, SUBCOMMITTEE ON INFORMATION, JUSTICE, TRANSPORTATION, AND AGRICULTURE

It is a pleasure to be here today with Chairman Don Edwards and other members of the Civil and Constitutional Rights Subcommittee for this joint hearing. Don Edwards is not only the dean of the California delegation, he is the dean of civil and constitutional rights on Capitol Hill. In that capacity, he has served as a watchdog for the National Crime Information Center for many years. It is a privilege to share the platform with him.

Our two Subcommittees share a common interest in the protection of personal privacy. That is what motivated the Subcommittee on Information, Justice, Transportation, and Agriculture, which I chair, to initiate a GAO investigation of NCIC. In December 1991, federal prosecutors in New Jersey and Florida brought indictments against private investigators and federal employees for illegally buying and selling confidential data from federal government computers, including NCIC. The indictments may only represent the tip of the iceberg.

There have been allegations for years of open trafficking in criminal history records derived from NCIC. Since so many law enforcement agencies and personnel have access to the NCIC computers, it is not difficult for a private detective or former policeman to find someone who is willing to provide a record for an improper purpose. Some private detective companies openly advertise their ability to obtain criminal history records. This is why GAO was asked to look specifically at the controls on access and use of NCIC.

GAO's testimony will be important for two distinct reasons. First, NCIC is a major repository of sensitive personal information. The system operates on a presumption that the data will only be used for legitimate law enforcement purposes, but GAO has found that the data is not adequately protected. NCIC is a vital resource for law enforcement, but the data must be protected against improper use.

Second, we can view NCIC as a model for any nationwide database of personal information with a large number of access points. Another information system with

similar characteristics is operated by credit bureaus. There are also widespread allegations and evidence that credit records are routinely used for purposes that are not permitted under the Fair Credit Reporting Act. The broader question is whether it is possible to operate any nationwide system containing personal information without opening the records to routine abuse.

These systems can be viewed as an attractive nuisance, just like a swimming pool near a school. Once built, we know with certainty that children who are not supposed to use the facility will try to do so anyway. In the case of a swimming pool, we can require that a fence be built. But for a data system, the issue is whether any fence or any procedure or any controls will work effectively to keep insiders from misusing data and to keep outsiders from buying access illegally.

And make no mistake about it. The principal threat comes not from hackers but from those people who have a legitimate right of access and who use that right for illicit purposes. It appears that there are employers, insurers, lawyers, or investigators who are willing to pay for illegal access to personal information, and there are some insiders who are willing to supply the data.

This is a very difficult problem, but one that we must face. The Internal Revenue Service is building a nationwide system for tax records. Health reform appears to be just around the corner, and it will certainly include greater computerization of health care records. My Subcommittee is in the process of drafting legislation that will address the confidentiality needs of health records. How will we be able to protect health records in a computerized environment if we can't adequately protect criminal history records or credit records? I hope to learn something by listening to GAO's findings about NCIC.

Let me make one additional point. No one should take comfort today because they don't have a criminal record. Don't assume that controlling use and disclosure of personal information is somebody else's problem. Everybody has a tax record or a credit record or a medical record. If we can't protect computerized records, then everyone is at risk. This is the general problem raised by today's hearing. I hope that we can find some answers.

PREPARED STATEMENT OF HON. CRAIG THOMAS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Mr. Chairman, the improper or unlawful use of computerized data is regrettably a subject we are going to hear more about. Nation-wide data bases are likely to proliferate as a quick and convenient way to access information. The new health care reform proposal the Administration will unveil this fall is one area in which national computerized records may be used.

With the easy access to these records, however, comes the opportunity for misuse of their information. As we will hear from GAO this morning, about 500,000 people have lawful access to the files in the FBI's National Crime Information Center. It is especially disturbing to learn that these "insiders," those with legitimate access, pose the greatest threat to NCIC security. Whether it is to gain information for personal use or to sell criminal history backgrounds for profit, NCIC users are too often tempted to abuse their access to NCIC files.

And the penalties for misusing NCIC data pale in comparison to the benefits one may gain by obtaining or selling this valuable information. Even if someone is caught abusing their NCIC access, the consequences have been limited mainly to administrative sanctions, since there are no federal or state statutes making misuse of NCIC information a crime. Clearly, there is much room for improvement here, and corrective action is sorely needed.

I commend both subcommittees for holding this hearing to look at the existing controls and vulnerabilities of the National Crime Information Center, with a view toward reducing improper use and disclosure of the information contained in NCIC files. I welcome our witnesses from GAO this morning, and I look forward to their testimony on the weaknesses in the NCIC system and opportunities for Congress to help the FBI improve the NCICs record in this area.

Thank you, Mr. Chairman.

Mr. EDWARDS. Will the witnesses please raise their right hands?

[Witnesses sworn.]

Mr. EDWARDS. Thank you very much.

Would you introduce the witnesses, Mr. Condit?

Mr. CONDIT. We have Laurie Ekstrand, Associate Director of the Administration of Justice Issues, General Government Division,

General Accounting Office. Why don't you introduce your colleagues for us today?

STATEMENT OF LAURIE E. EKSTRAND, ASSOCIATE DIRECTOR, ADMINISTRATION OF JUSTICE ISSUES, GENERAL GOVERNMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY DAN HARRIS, ASSISTANT DIRECTOR, LAW ENFORCEMENT MATTERS; SETO BAGDOYAN, EVALUATOR IN CHARGE; AND MATTHEW VILLARREAL, EVALUATOR

Ms. EKSTRAND. Thank you, I would be glad to.

On my immediate left is Dan Harris, Assistant Director in Administration of Justice in the Washington office. On my immediate right is Seto Bagdoyan, he was the evaluator in charge for this work. He is in our Los Angeles regional office. To my far right is Matthew Villarreal, he is an evaluator and worked on this work from our Los Angeles regional office.

Mr. CONDIT. Thank you.

We are delighted that you're all here this morning and we want to begin with your testimony, please.

Ms. EKSTRAND. Thank you.

Mr. Chairman——

Mr. EDWARDS. Will you bring the mike up as close to your mouth as you can, please?

Ms. EKSTRAND. Certainly.

I am pleased to be here today to testify about the work we did at the request of the chairman of the Subcommittee on Information, Justice, Agriculture, and Transportation, House Government Operations Committee, on the Federal Bureau of Investigation's National Crime Information Center. NCIC is the Nation's most extensive criminal justice information system and provides user agencies with information on items such as missing and wanted persons, stolen vehicles, and criminal history records.

Currently, NCIC contains over 24 million records in 14 files. Over 19,000 law enforcement and other criminal justice agencies in the United States and Canada can access NCIC directly through their computer systems.

An additional 51,000 agencies can access NCIC indirectly through user agreements with agencies that have direct access. Federal regulations and NCIC policy have classified NCIC information as sensitive and have restricted access to and use of the information to authorized criminal justice agencies for purposes such as conducting criminal investigations or screening applicants for employment in criminal justice positions.

In December 1991, 20 individuals in New Jersey and Florida were indicted under Federal theft of government property, computer fraud, and bribery statutes for the sale of criminal history information from NCIC. The subcommittee viewed these indictments as support for general allegations that NCIC information is routinely made available for unauthorized purposes by some Federal, State, and local law enforcement agencies.

Citing these allegations, the chairman of the subcommittee requested that we review NCIC to determine if the system has adequate controls to prevent misuse, and obtain any FBI and State assessments of the extent and nature of NCIC misuse and examples

of such misuse. To fulfill the request, we interviewed officials from the FBI and the 54 State agencies who oversee local user agencies; we visited user agencies in California, Nevada, and Texas; and we reviewed relevant documentation.

We found that NCIC is vulnerable to misuse from individuals with authorized access, or insiders, because of the system's inherent risk and the inadequacy and ineffectiveness of some controls in State criminal justice information systems through which users access NCIC.

Specifically, NCIC is inherently risky because, number one, its security policy is too broad and contains only minimum requirements and does not require specific controls. This results in State systems with different controls. Two, its many users generate a large number of transactions. Three, the information contained in the files is valuable and in demand, and has been used for unauthorized purposes. Four, the incentives for misuse outweigh the potential penalties. And five, misuse has been repeatedly reported in FBI and State audits.

The controls of some State systems accessing NCIC are not adequate because they lack unique individual user identification, authentication, and accountability. Other controls, such as audit trails and biennial audits of user agencies, are not being used effectively.

For example, audit trail information is not being reviewed frequently by many user agencies as a means to detect misuse. Furthermore, the FBI and 16 State agencies responsible for oversight of local user agencies are not meeting the requirement to biennially audit the State and local agency respectively.

Since NCIC is a network of coordinated State systems, and the same information can be accessed from any one of these systems, the control limitations of one system, combined with NCIC's inherent risk, render the entire network vulnerable to misuse.

While the security features of the upgraded NCIC 2000 system are a step in the right direction to address the system's vulnerability, potential limitations of their capacity and implementation could diminish their effectiveness. Most significant of these limitations is that States will not be required to implement NCIC 2000's security features.

A conference of NCIC users and contractors this fall is in part intended to address technical and implementation issues. We believe that this is a good forum in which to also discuss the capability and implementation issues we have identified.

We could not obtain an overall assessment of the extent and nature of NCIC misuse because the FBI and most State oversight agencies do not systematically maintain statistics or other information on misuse incidents. We did, however, obtain 62 examples of such misuse from the FBI and some States.

These examples showed that NCIC has been misused intentionally, such as disclosing information to private investigators in exchange for money, and unintentionally, such as conducting background investigations on applicants for noncriminal justice employment. The examples also showed that individuals responsible for misuse generally have not been criminally prosecuted because of the lack of applicable Federal and State statutes.

For example, only seven individuals in our 62 examples were criminally prosecuted. Instead of being prosecuted, most individuals have received administrative sanctions, ranking from reprimands to termination of employment.

We believe that on the basis of our findings, misuse of NCIC is a problem which needs to be addressed more effectively. We emphasize that any measure aimed at making such misuse less likely can be effective only if implemented in a coordinated manner with others.

For example, if NCIC 2000's security features are implemented and consequently detect more incidents of misuse, directly applicable legislation will be needed to ensure that individuals responsible are prosecuted. On the other hand, while legislation may help prosecute some detected violators, without the additional security measures some misuse may go undetected.

We recommend that Congress enact legislation with strong criminal sanctions specifically directed to the misuse of NCIC. Such legislation could be aimed at deterring individuals contemplating misuse of NCIC, and facilitating and encouraging prosecution of individuals who have misused NCIC.

In view of our findings and the NCIC 2000 implementation, we also recommend that the Director of the FBI and the NCIC Policy Advisory Board reevaluate the security specifications set forth in the NCIC security policy, particularly in the area of accountability. Recognizing the potential cost and implementation concerns involved, at a minimum, the FBI and the Advisory Policy Board should amend the security policy to endorse and encourage States and local user agencies to enhance their security features, such as increasing user accountability through identification, authentication, and audit, to meet the C2 security rating of NCIC 2000.

Justice Department and FBI officials reviewed a draft of our testimony and agreed with our findings, conclusions, and recommendations. According to these officials, Federal legislation will be very helpful to deter insiders from misusing NCIC.

This concludes my opening statement. But in closing I would like to acknowledge the cooperation of the FBI and State and local law enforcement officials during the course of our review.

We would be very happy to answer any questions you may have.

[The prepared statement of Ms. Ekstrand follows:]

PREPARED STATEMENT OF LAURIE E. EKSTRAND, ASSOCIATE DIRECTOR, ADMINISTRATION OF JUSTICE ISSUES, GENERAL GOVERNMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to testify about work we did at the request of the Chairman of the Subcommittee on Information, Justice, Agriculture, and Transportation, House Government Operations Committee, on the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC). NCIC provides federal, state, and local law enforcement and other criminal justice agencies with information on items such as missing and wanted persons and stolen vehicles and other property. NCIC also provides criminal history record information on individuals through its largest file, the Interstate Identification Index (III). Federal regulations and NCIC policy have classified NCIC information as sensitive and have restricted access to and use of such information to authorized criminal justice agencies for criminal justice purposes. These purposes include conducting criminal investigations or screening applicants for employment in criminal justice positions.

In December 1991, 20 individuals in New Jersey and Florida were indicted under federal bribery, theft of government property, and computer fraud statutes[1] for selling criminal history information obtained from NCIC. The Subcommittee viewed these indictments as support for general allegations that NCIC information is routinely made available for unauthorized purposes by some federal, state, and local law enforcement agencies. Citing these allegations, the Subcommittee requested that we (1) determine whether the FBI and user agencies have adequate controls to ensure access to NCIC is for authorized purposes, and deter and detect misuse[2] of NCIC information; and (2) obtain the FBI's and the states' assessments of the extent and nature of any NCIC misuse and examples of such misuse.

To fulfill the Subcommittee's request, we interviewed FBI officials responsible for NCIC; reviewed NCIC and state and local agency security and other relevant documentation; and visited state and local law enforcement agencies who use NCIC in California, Nevada, and Texas and interviewed relevant officials from these agencies. We did this work to obtain a description of the system and its controls and to learn how it operates. We also observed the physical security of NCIC terminals at the locations visited and the controls and safeguards for accessing and disseminating information from the system.

In addition, we did a telephone survey of all 54[3] state control terminal agencies (SCTA) that oversee local user agencies in the United States and Canada to obtain information on state and local agency access to NCIC; access and dissemination controls; and the extent of unauthorized disclosure and use of NCIC information. We administered our survey between January 25 and February 18, 1993. We did not verify the accuracy of the information provided during the survey.

Finally, to obtain assessments of NCIC by computer security experts, we reviewed an NCIC risk analysis by MITRE Corporation prepared for the FBI in 1989; a report by Computer Professionals for Social Responsibility prepared for the Subcommittee on Civil and Constitutional Rights, House Judiciary Committee, in 1989; and a report by SRI International (formerly Stanford Research Institute) prepared for the FBI in 1990. We also interviewed the author of the SRI report. A more complete description of our scope and methodology appears in Appendix I.

BACKGROUND

NCIC is the nation's most extensive computerized criminal justice information system. The system consists of a central computer at FBI headquarters in Washington, D.C.; dedicated telecommunications lines; and a coordinated network of federal and state criminal justice information systems. NCIC provides users with access to over 24 million records in 14 files, such as files on wanted persons, stolen vehicles, and missing persons. NCIC's largest file, the III file, provides access to about 17 million criminal history information records contained in state systems.

Because it is a cooperative effort between the federal government and the states, NCIC is a decentralized system. Specifically, the NCIC Advisory Policy Board (APB), which is composed of managers of state and local user systems, is responsible for establishing and implementing the system's operational policies, including security. The FBI is responsible for overall management of NCIC. The 54 SCTAs, through agreements with the FBI, are responsible for maintaining their state's criminal justice information systems through which local user agencies access NCIC. The SCTAs also are responsible for overseeing the federal, state, and local user agencies in each state.

Over 19,000 federal, state, and local law enforcement and other criminal justice agencies in the United States and Canada can access NCIC directly. About 97,000 computer terminals in these agencies can access NCIC. An additional 51,000 law enforcement and other criminal justice agencies can access NCIC indirectly through agreements with user agencies that have direct access. More than 500,000 individuals within the user agencies can access NCIC, either directly from their own computer terminals or indirectly through computer terminal operators.

The Originating Agency Identifier (ORI), a nine-character code assigned by the FBI to each user agency, is the primary control for accessing NCIC. The ORI controls user agency access to NCIC by identifying each agency to the system and determining the levels of access to NCIC files and types of functions allowed, such as inquiries and requests for records.

---

[1] 18 U.S.C. 201, 18 U.S.C. 641, and 18 U.S.C. 1030.

[2] Misuse refers to access to, and disclosure and use of, NCIC information for unauthorized purposes, such as background investigations for noncriminal justice employment.

[3] This number represents the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and Canada.

NCIC IS VULNERABLE TO MISUSE

NCIC is vulnerable to misuse because of its inherent risk and the inadequacy and ineffectiveness of some of its controls. Individuals with authorized access, or "insiders," pose the greatest security threat to the system. Since NCIC is a network of coordinated state systems and the same information can be accessed from any one of these systems, the control limitations in one system render the entire network vulnerable to misuse. While NCIC 2000's security features are a positive development in the effort to address the system's vulnerability, potential limitations in their capabilities and implementation could diminish their effectiveness.

Insiders Are the Greatest Security Threat to NCIC

A 1989 NCIC risk analysis by MITRE Corporation concluded that insiders were the greatest security threat to NCIC. Another security expert, who has studied NCIC, and FBI and SCTA officials we spoke with also identified the insider as the greatest security threat to NCIC. These sources indicated that insiders pose the greatest threat to NCIC because they know the system and can misuse it by obtaining and selling information to unauthorized individuals, such as private investigators, or altering or deleting information in NCIC records. Insiders can access NCIC either by pretending they are involved in legitimate law enforcement activity, or by masquerading their real identity when identifying themselves to the system.

NCIC Is Inherently Risky

NCIC is inherently risky[4] because (1) its security policy is too broad, contains only minimum requirements, and does not require specific controls, thus resulting in state systems with different controls; (2) its many users generate a large number of transactions; (3) the information contained in its files is valuable and in demand and can be used for unauthorized purposes; (4) the incentives for misuse outweigh the potential penalties; and (5) misuse has been repeatedly reported in FBI audits.

NCIC Security Policy Is Too Broad and Contains Only Minimum Requirements

According to the GAO policy guide criteria for determining inherent risk, vague regulations contribute to such risk. Even though the NCIC APB regards the *NCIC Security Policy* as a comprehensive document, the Policy is too broad and contains, by its own acknowledgement, only minimum requirements for NCIC security in six general areas: (1) background screenings of employees and discipline standards for policy violators; (2) physical security and access to NCIC terminals; (3) authorization and oversight of user agencies; (4) technical safeguards, such as automated audit trails; (5) dissemination of NCIC information; and (6) biennial audits of local users to measure compliance with NCIC policies. While the Policy allows the SCTAs to establish stricter requirements at their discretion, it does not require specific access controls.

Specific access controls not required

While the NCIC Security Policy requires some minimum controls, it does not require specific controls, such as unique passwords or identifiers, to control access and identify authorized users. According to FBI officials and a computer security expert, the Policy does not require such controls because of potential resistance by the states to federal encroachment on their sovereignty, restrictions imposed by state security policies, and the lack of funding to implement passwords and other controls. In addition, FBI officials stated that since most NCIC files do not contain sensitive information, they may not require additional protection. However, this position seems to be inconsistent with the fact that the Policy has classified all information in the system as sensitive and in need of protection.

The Security Policy's position on access controls and identifiers also appears to be inconsistent with the fact that insiders have been identified as the greatest security threat to NCIC. In this regard, there is no requirement to identify such individuals through unique identifiers that cannot be compromised. While the Policy requires that automated audit trails identify the terminal operator, requester, and secondary recipient of III file information "in some way," including name, badge or serial number, or other unique number, such identifiers are not confidential, nor are they monitored by NCIC's central computer. Insiders can use identifiers that are not confidential to disguise their identities and prevent their identification in audit trails.

---

[4] To determine NCIC's inherent risk, we used criteria contained in a GAO policy guide titled *Asessing Compliance With Applicable Laws and Regulations*, (GAO/OP-4.1.2, Dec. 1989). This guide supplements the *Yellow Book* standards on internal controls.

Furthermore, the data fields that record such identifiers can sometimes be bypassed, either by entering erroneous data, or simply using the space bar on a computer terminal's keyboard to exit the data fields without entering any data. For example, a user, or users, in a law enforcement agency in Texas were able to disguise their identity by using the name of a former employee of that agency and the names of months. Users in another law enforcement agency in Texas were able to bypass an identification data field by entering letters such as "XYZ," while users in an agency in Nevada were able to bypass an identification data field by using the keyboard space bar.

Computer security experts have determined that unique identifiers are important for user identification, authentication, and accountability. Unique identification is the process through which individuals identify themselves to a computer system. Authentication is the process of ensuring that the identification provided to the system is likely to be correct. Accountability combines authentication with the review of audit trail information to trace a sequence of events in a computer system back to a specific individual. According to a computer security expert and Department of Defense computer security criteria, these three steps in combination are the most fundamental requirements for deterring and detecting misuse and enhancing computer system security.

State systems use different types of access controls

Since the NCIC Security Policy does not require specific access controls, state systems use different types of controls for accessing NCIC. For example, systems such as those in Alabama, Arizona, California, and Texas use computer terminal configurations, sometimes called "security tables," to control access to NCIC. These configurations control which individuals can access NCIC, the types of information they can access, and the functions they can perform. For example, a terminal operator may be authorized to access all NCIC files except the III file, which contains criminal history information. Within the files accessed, this individual may be authorized to perform only inquiries. State systems such as those in Illinois, Nebraska, and Washington use ORIs in terminal configurations to identify users accessing NCIC and control access to the system's files.

Although not required by the Security Policy, some state systems also use passwords or other identifiers to control access to NCIC. Specifically, only 19 systems require unique or general passwords or identifiers to access NCIC. However, it should be noted that 30 state systems require either unique or general passwords or identifiers for initial access to these state systems through which local user agencies access NCIC. Some state systems, such as those in Maryland and New York, use passwords or other identifiers in combination with terminal configurations to control access to NCIC. The FBI also uses passwords to control access to NCIC. However, the FBI requires passwords only for accessing NCIC from terminals located in its headquarters, while FBI field offices adhere to password and other security policies established by the states in which they are located. According to FBI officials, they do not have influence over the establishment and implementation of state security policies.

Most state systems use automated audit trails to track NCIC user activity and the dissemination of criminal history information. The Security Policy requires that audit trail information be maintained for a minimum of 1 year for the III file. To meet this requirement, states maintain III file audit trail information for different lengths of time. For example, states such as Colorado, Kentucky, and Wyoming maintain audit trail information for a minimum of 1 year, while states such as Montana, Virginia, and Washington maintain such information indefinitely. The FBI maintains NCIC audit trail information for 10 years

The minimum requirements in the Security Policy, which do not call for specific access controls, have allowed the states to implement relatively simple controls, such as computer terminal configurations, for their own systems and still meet these minimum requirements. Furthermore, since NCIC is a network of coordinated state systems and the same information can be accessed from any one of these systems, simple controls in some systems compromise the entire network and render it vulnerable to misuse. For example, an employment firm obtained III file information from a law enforcement agency in Georgia. However, when this activity was discovered in Georgia, the firm began using a law enforcement agency in South Carolina to obtain the same information.

NCIC Users Generate Large Numbers of Transactions

According to the GAO policy guide criteria, the more transactions there are involved in an activity, the greater the chances of noncompliance with policies due to errors, irregularities, and abuse. This is especially true if the activity is delegated

outside the government's control, in this case to the SCTAs and local user agencies, without active monitoring or oversight. Furthermore, the large number of transactions increases the difficulty of detecting such abuse. FBI, SCTA, and local user agency officials told us that the large number of transactions generated by NCIC's users makes it easier for insiders misusing the system to disguise their activities and more difficult for the system's audit trails to detect these activities.

In this regard, since NCIC is the nation's most extensive criminal justice information system, the more than 70,000 agencies and 500,000 individuals who use the system generate a large number of transactions, including inquiries and requests for records. The number of NCIC transactions has increased significantly since 1967, when the system became operational. Specifically, in 1992 NCIC users generated about 438 million transactions, or about 1.2 million a day, compared to about 2 million transactions in all of 1967. Over 28 million of the 1992 transactions involved NCIC's III file.

NCIC Information Is Valuable and Has Been Used For Unauthorized Purposes

According to the GAO policy guide criteria, assets such as NCIC information that are readily marketable or could be used for personal purposes are very susceptible to improper use and contribute to a system's inherent risk. Federal regulations[5] and the NCIC Security Policy regard NCIC information as sensitive and generally restrict access to and use of such information to authorized criminal justice agencies for criminal justice purposes. These purposes include conducting criminal investigations and screening applicants for criminal justice employment, or, through special agreements with authorized federal agencies, for granting security clearances.

However, in addition to its legitimate uses, information contained in NCIC's files is valuable and has been used by insiders for unauthorized purposes. Specifically, the examples of misuse we obtained in our review showed that insiders used NCIC information for personal purposes, such as determining whether friends or relatives had criminal records, or sold it to private investigators who used the information to conduct background investigations on applicants for employment. Furthermore, during a July 1992 congressional hearing on the sale of criminal history records, FBI officials testified that there was a demand for NCIC information because such information is valuable to individuals other than criminal justice professionals, including private citizens, employers, parents, and politicians.

Incentives For Misuse Outweigh Potential Penalties

According to the GAO policy guide criteria, certain characteristics of a system, such as incentives for misuse, increase the susceptibility to noncompliance and thus contribute to inherent risk. In this regard, the examples of NCIC misuse we obtained showed that the incentives for such misuse, such as personal gain or money, may have outweighed the potential penalties. As discussed later, there are no federal or state statutes specifically directed at misuse of NCIC. In the majority of cases, the penalties for such misuse have in the past been limited to administrative sanctions, such as written or oral reprimands, suspensions, or termination of employment.

During the July 1992 congressional hearing, FBI officials also testified that existing federal statutes have not been adequate to deter misuse of NCIC because the market for its information is too lucrative. Individuals are willing to pay to obtain NCIC information, even though they are not authorized to receive it.

Misuse Repeatedly Reported in User Audits

According to the GAO policy guide criteria, the repeated disclosure of problems in audits is a factor in assessing the inherent risk of a system. Our review of audits of NCIC user agencies, conducted by the FBI, showed that misuse of NCIC, such as using the system to conduct background investigations of applicants for noncriminal justice employment, and other incidents of noncompliance with NCIC policy were repeatedly reported.

More specifically, our review of FBI audits of SCTAs showed that 46 SCTAs had not corrected misuse and other problems identified during the most recent audits. Uncorrected problems included using the III file for noncriminal justice purposes, not meeting the biennial audit requirement, and not implementing training programs. Six SCTAs had corrected problems identified during previous audits. Audit reports for Canada and the U.S. Virgin Islands were not available.

[5] 28 C.F.R., Chapter I, Part 20, Section 20.33.

Some NCIC Controls Are Either Not Adequate or Are Not Being Used Effectively to Deter or Detect Misuse

Office of Management and Budget Circular A-130 establishes policy guidance for systems like NCIC. More specifically, the circular requires that agencies establish a level of security commensurate with the sensitivity of the information and the risk and magnitude of the loss or harm that could result from the improper operation of the system. The guidance further indicates that for applications considered sensitive, the management control process shall, at a minimum, include security specifications and design review and system tests. It further advises that the tests ensure that administrative, technical, and physical controls are operationally adequate. While the NCIC Security Policy includes security specifications, as discussed below, the controls in some state systems in the NCIC network are not adequate, nor are they being used effectively to promote a level of security that effectively detects and deters misuse. The control limitations, combined with NCIC's inherent risk, could increase the system's vulnerability to misuse.

Access Controls of Some State Systems Are Not Adequate

The access controls of some state systems are not adequate to deter and detect misuse of NCIC, even though these controls appear to meet the minimum requirements of the NCIC Security Policy. The controls are not adequate because they lack unique individual user identification, authentication, and accountability. For example, SCTA officials from Arizona, Michigan, New York, and Washington cited as a weakness in their systems accessing NCIC the lack of user identification and accountability. As discussed earlier, computer security experts have emphasized that identification, authentication, and accountability are essential in deterring and detecting misuse of computer systems.

We found that security controls in state systems could be adversely affected by the lack of unique user identification. Specifically, the most commonly used control, terminal configurations, are not adequate to control access if users do not use unique identifiers. According to a computer security expert, while ORIs are used as identifiers, they often identify only the agency, rather than individual users or terminals. For example, the Los Angeles Police Department had over 1000 terminals with which to access NCIC but presented only 1 ORI to the system. Insiders seeking to misuse NCIC can use systems such as this without disclosing their identity. For example, a police officer conducted background searches on an individual from a court terminal, instead of his own, seeking to disguise his identity. The state in which this incident occurred does not require unique or general passwords or other identifiers for accessing NCIC. Instead, access to NCIC is controlled by a terminal identifier and an agency ORI. The officer was detected because the subject of his searches complained.

The lack of unique identifiers in state systems can also affect accountability in audit trails. Specifically, 17 state system audit trails do not identify the individual accessing NCIC, but only the terminal from which a transaction originated, thus potentially hindering the identification of those responsible for misuse. According to computer security experts, user identification is essential for audit trails because they are the last recourse for detecting and identifying those misusing NCIC. For example, SCTA audits of five large law enforcement agencies in Texas, a state which does not require a unique password or other identifier to access NCIC, determined that these agencies' audit trails were not recording the identities of terminal operators, or, in some cases, the identities of requesters of criminal history record information, making the identification of those responsible for misuse virtually impossible.

Insiders who know the state systems and their control weaknesses, can take advantage of inadequate controls to access the system by using false identities, also known as masquerading. For example, a terminal operator in a sheriff's office in Texas accessed NCIC using fictitious identifiers and used the information he obtained for unauthorized purposes. An ensuing investigation could not conclusively determine the nature of these purposes.

In contrast, we found several examples of state systems with relatively more extensive controls for accessing NCIC. These controls emphasized user identification, authentication, and accountability. For example, one state system required a unique operator identifier to access NCIC. This identifier consisted of one alphabetic character, operator social security number, and an optional eight-character identifier. Another state system required a terminal identifier, an individual access code, and an individual password to access NCIC. In addition, the system required a system-wide access code and password to access NCIC's III file.

Some Existing Controls Are Not Being Used Effectively

Some existing controls, specifically audit trails and biennial audits, are not being used effectively to detect or deter NCIC misuse. On the basis of our discussions and telephone survey, we found that the FBI and 25 of the SCTAs review audit trail information only during the biennial audits of SCTAs and local user agencies. According to FBI and SCTA officials, they do not review such information more frequently because of the large number of transactions generated by users and staff shortages. The lack of frequent reviews of audit trail information may result in significant incidents of misuse not being detected. For example, according to FBI officials, even though transactions related to the misuse were recorded in audit trails, the most significant case of NCIC misuse was detected through an anonymous tip. The FBI was alerted about the misuse when a price list was mailed to a federal agency advertising the availability of government information, including NCIC information. The FBI investigated this incident and then, using audit trail information, uncovered an extensive network of insiders misusing NCIC.

In contrast, 16 SCTAs contacted in our telephone survey told us that they review audit trail information more frequently than during biennial audits. These SCTAs review such information either daily, weekly, monthly, quarterly, or annually. For example, one SCTA official described an extensive security program for NCIC that includes monthly reviews of audit trail information. The monthly review of such information seeks to detect unusual or suspicious levels of activity by individual terminal operators. In addition, the security program includes unannounced security visits to local user agencies where audit trail information is also reviewed, and the required biennial audit of local user agencies. According to this official, the security program has been successful and there have been very few incidents of NCIC misuse since its inception. He described one incident in which the review of audit trail information detected the most significant case of NCIC misuse in his state. Specifically, the review detected a law enforcement officer who was conducting background searches on individuals seeking employment with a nationally known firm. In another example, an SCTA official also described an incident in which the weekly review of audit trail information detected a police dispatcher who was conducting background searches on her fiance's political opponents.

The NCIC Security Policy requires that the SCTAs biennially audit local user agencies, and that the FBI biennially audit the SCTAs. Our survey and discussions with FBI and some SCTA officials showed that they are not meeting the biennial audit requirement, mainly because of staff shortages, budget constraints, and the large numbers of agencies to be audited. Specifically, according to an FBI official, the FBI is able to audit the SCTAs only every 30 months, while, according to our survey, 16 SCTAs are able to audit local user agencies only every 30 to over 48 months. The delays of the FBI audits could continue, given the staffing shortages at the Bureau's Criminal Justice Information Systems Division. Our survey found that 36 SCTAs currently comply with the biennial audit requirement—2 SCTAs did not know if they were complying with the requirement. Delays of these audits beyond the 2-year requirement may prevent the timely detection of NCIC misuse. Furthermore, the review of such information during the biennial audits of user agencies who maintain audit trail information only for 1 year would not reveal any misuse that may have occurred more than a year from the time of the audit.

The FBI and SCTAs use these audits of user agencies to evaluate the effectiveness of system controls and to measure compliance with NCIC policies. However, during our telephone survey, only 45 SCTAs reported using these audits as a means to detect misuse of NCIC, usually by sampling audit trail information. Similarly, the NCIC Security Policy does not require a specific audit step to detect misuse.

NCIC 2000 Attempts to Address Security Concerns, But Potential Limitations Could Diminish Effectiveness

In 1986, the FBI began planning to upgrade the current NCIC system. The proposed upgraded system, called NCIC 2000, will be composed of a Central Segment at FBI headquarters, workstations for user agencies, and mobile imaging units for patrol cars. NCIC 2000 will provide new system software and additional capabilities, including receiving, storing, and transmitting images of persons and property and analyzing digitized fingerprints. The contract for NCIC 2000 was awarded in March 1993 to Harris Corporation. The FBI expects to implement its segment of NCIC 2000 by March 1995, while the states are required to be operationally capable by March 1998.

In an attempt to address concerns about security, NCIC 2000 is to also include certain security features that the current system does not have. According to FBI officials, the features are based on findings and recommendations of a 1989 NCIC

risk analysis by MITRE Corporation and a 1990 report by SRI International on security controls for computer systems accessing NCIC. NCIC 2000's Central Segment and workstations will have the Department of Defense's C2 and D2 security ratings respectively.[6] Specific security features of the Central Segment include access control, a data encryption system to protect data transmissions from outside intruders (hackers); and a knowledge-based intrusion detection system designed to detect unusual, and potentially unauthorized, levels of user activity based on established usage patterns, called "user profiles."

We believe that while the planned security features may ultimately be helpful in improving NCIC's security, their potential limitations and limited implementation could diminish their effectiveness. The author of the SRI report, while acknowledging that the FBI is making a good effort to address his report's recommendations, also stressed that NCIC 2000 will remain vulnerable to misuse because of the security features' potential limitations and their limited implementation, particularly at the state and local levels.

Potential Limitations of Security Features

NCIC 2000's security features have potential limitations that could diminish their effectiveness. According to SCTA officials, while the security features may reduce NCIC 2000's vulnerability, the threat to the system from insiders will remain. For example, the Chairman of the NCIC APB told us that the threat from insiders will always be present in a system like NCIC because of both its nature and the number of users with authorized access.

According to FBI officials, the system's Central Segment will provide only limited security for the state systems. For example, it will provide accountability only to the ORI level by identifying the user agency accessing the system, rather than to the individual user level. Furthermore, according to a computer security expert, a C2 security rating would be only a minimum starting point for systems accessing NCIC, with evolution to some of the requirements of higher ratings to further improve security.

According to FBI officials, the data encryption feature will encrypt only data transmitted between the FBI and state systems. The same data will not be encrypted when transmitted from the state systems to local user agencies, leaving the data still vulnerable to potential hackers. One of these officials questioned the need for encryption because NCIC data are already unreadable during their transmission through dedicated communication lines. According to this official, it would be very costly, time consuming, and difficult for hackers to access NCIC data during transmission. It would be more cost effective for such individuals to obtain information from NCIC through an insider. In addition, hackers have not been identified as primary security threats to NCIC. In this regard, none of the examples of NCIC misuse we obtained during our review involved hackers.

According to FBI officials and a computer security expert, the intrusion detection system also has potential limitations. First, according to an FBI official, each individual user will not have a user profile. Instead, groups of users, such as dispatchers and detectives, would have group profiles. Second, individual incidents of misuse, unlike high-volume patterns of such incidents,may not be detected because they may not appear to be all that unusual. In fact, according to an FBI official, the system will primarily detect data input errors and only the most blatant violations. Furthermore, according to a computer security expert, the system will not detect occasional misuse by an insider, but only repeated transactions not authorized for a user agency or the most obvious violations, such as an individual attempting to download an entire NCIC file. Third, the FBI plans to monitor user activity through the Central Segment's own intrusion detection system and alert specific agencies when unusual activity is detected. However, an FBI official acknowledged that given the shortage of FBI personnel in its Criminal Justice Information Systems Division, which is responsible for NCIC, it will be very difficult to adequately monitor and report user activity.

Limited Implementation of Security Features

As currently planned, only the FBI will implement the NCIC 2000 workstations at its headquarters, including the security features, to access the system. According to FBI officials, the states will be offered the opportunity to buy standardized

[6] C2-level security includes individual identification and authentication, access control, and audit. D2-level security includes similar features adapted for personal computers.

workstation packages, including the security features, to access NCIC 2000. However, the states will not be required to purchase the workstations because of potential incompatibility with their own computer systems and limited funding. FBI officials estimated the cost to outfit all users with workstations at about $2 billion. To access NCIC 2000, the states will either have to buy the workstation packages, buy and modify them to fit their own systems, or develop their own workstations. Twelve SCTA officials we contacted subsequent to our telephone survey told us that they would either fully implement NCIC 2000 by purchasing through the FBI procurement, modify FBI workstations to be compatible with their states' systems, or develop or modify their own systems to provide the required capability.

When developing their own workstations, the states will also not be required to include NCIC 2000's security features because of funding and system compatibility considerations. Furthermore, according to the FBI, there is no incentive for the states to comply with NCIC 2000 security features. Specifically, as currently planned, the NCIC Security Policy will not be modified to require compliance with NCIC 2000 standards, nor will the states receive financial support for implementing the system. In addition, according to FBI officials, there are no sanctions that the FBI can realistically impose on the states for such noncompliance. For example, revoking a state's access to NCIC would be counter to the system's mission of assisting law enforcement agencies. However, in our follow up to the survey, several of the SCTA officials we contacted told us that they would implement some of the security features, such as data encryption or passwords, if funding becomes available.

The 12 SCTA officials we contacted also identified certain barriers that may affect the overall implementation of NCIC 2000. First, funding shortages may prevent local user agencies from fully implementing the new system. For example, in one state, local user agencies will not be required to purchase imaging units or fingerprint scanners, while in another state all local user agencies may not immediately implement the mobile imaging units. Second, hardware and software compatibility problems may delay implementation. For example, one SCTA official told us that some hardware and software compatibility problems will delay implementation, making it more difficult to meet the 5-year deadline. Third, staff shortages at the FBI's Criminal Justice Information Systems Division will affect training and other technical assistance to the states. The Chairman of the NCIC APB also said that training will be an issue in every state.

A conference of NCIC users and contractors, scheduled for this fall, is in part intended to address capability and implementation issues for NCIC 2000. We believe that this will be a good forum to discuss and resolve some of the capability and implementation issues we have identified.

EXTENT AND NATURE OF NCIC MISUSE CANNOT BE ASSESSED BUT INCIDENTS OF MISUSE HAVE OCCURRED

We could not obtain FBI and state assessments of the extent and nature of the misuse of NCIC because the FBI and most SCTAs do no systematically maintain statistics or other information on incidents of misuse. We were, however, able to obtain general information on the extent and nature of NCIC misuse and specific examples of such misuse from the FBI, our review of FBI audits of SCTAs, our visits to SCTAs, and our telephone survey of SCTAs.

FBI and Most SCTAs Do Not Maintain Statistics or Adequate Information on Misuse Incidents

FBI officials could not provide us with a statistical assessment of the extent and nature of NCIC misuse because they do not maintain statistics or other adequate information on such incidents. Of the 54 SCTA officials we interviewed during our telephone survey, 41 expressed the opinion that misuse in their states was a problem to some or little extent, 12 to no extent, and 1 to a moderate extent.[7] However, many of these officials could not provide any statistical or other evidence to support their assessments. Specifically, only 22 SCTAs maintained statistics on misuse incidents, while 32 SCTAs did not maintain any statistics. Furthermore, 21 of 54 SCTA officials stated that their systems' controls were moderately effective in detecting misuse, while 8 stated that they were effective to some or little extent, and 1 to no extent. Thus, these self-assessments may underestimate the extent of the misuse problem.

According to the FBI and 21 SCTA officials, they do not maintain statistics on misuse incidents because there is no policy requirement to report and track incidents of misuse, or they did not believe it was necessary to collect such information,

[7] Our five-level survey scale ranged from "no extent" to "very great extent."

given the small number of misuse incidents that occur within their jurisdictions. Some SCTA officials are generally aware of significant misuse incidents in their states and maintain information about these incidents. For example, the Texas and New Mexico SCTAs maintain information about significant misuse incidents that are reported by local user agencies.

Examples Show NCIC Misused Intentionally and unintentionally

Even though we could not obtain an overall assessment of the extent and nature of NCIC misuse, we did obtain some general information about the extent and nature of such misuse from the FBI, SCTAs, our visits to user agencies, and our review of FBI audits of SCTAs. Specifically, the FBI reported that its Office of Professional Responsibility had investigated a total of eight incidents of NCIC misuse by FBI personnel during 1990 through 1992. Furthermore, our telephone survey showed that 12 SCTAs that maintained statistics on misuse incidents detected 159 such incidents in fiscal year 1992. It should be noted, however, that 100 of these incidents were detected by a single SCTA. In addition, 17 SCTAs that did not maintain statistics, still informed us that they were aware of 94 misuse incidents in their states. The misuse incidents were detected primarily through FBI or SCTA audits, tips from informants, complaints from victims of misuse, reviews of NCIC audit trail information, or by other means. Finally, our review of FBI audits of SCTAs showed that misuse incidents were detected in 58 law enforcement agencies in 30 states.

The FBI and SCTAs were able to provide some information on 62 of the examples of NCIC misuse. We found that 56 examples we obtained involved what we characterized as intentional and 6 involved unintentional misuse of NCIC. Furthermore, all of them involved insiders and none involved outside hackers. It should be noted that these examples were provided to us verbally and mostly without supporting evidence. Consequently, we could not verify the accuracy of these examples. Furthermore, the outcomes of five cases are still pending and the outcomes of eight cases are unknown. Finally, two examples involved an unknown number of additional misuse incidents. (See appendix II for all the examples of misuse we obtained.)

Intentional Misuse of NCIC

Fifty-six examples of misuse we obtained involved the intentional misuse of NCIC. Of these, 41 examples involved insiders using NCIC information either for personal purposes, such as determining whether friends, neighbors, or relatives had criminal records or political purposes, such as inquiring about the backgrounds of political opponents. In certain cases, the misuse of NCIC information jeopardized the safety of citizens and potentially of law enforcement personnel. In one extreme example, a former law enforcement officer in Arizona obtained NCIC information from three other officers and used it to track down his girlfriend and murder her. After an investigation, the three officers who provided the information were prosecuted, convicted, and sentenced to prison under Arizona state law. In another example, a terminal operator in Pennsylvania conducted background searches for her boyfriend, who was a drug dealer. He asked her to check the criminal history records of new clients to determine if they were undercover drug agents. She continued her activity until supervisors detected an unusual number of inquiries from her terminal.

An additional 16 incidents of intentional misuse involved insiders obtaining NCIC information and disclosing it to unauthorized persons, such as private investigators, in exchange for money or other rewards. In two such incidents, private investigators obtained and used NCIC information to conduct background investigations on individuals seeking employment with nationally known firms. In one example, a law enforcement officer in Alabama used NCIC to conduct background investigations for a national transportation firm. In another example, a private investigator in Texas obtained NCIC information from the chief of a small suburban police department to conduct background investigations for a restaurant chain and a computer firm. It is not known if these firms were aware that the use of NCIC in these investigations was a violation of NCIC policy.

Unintentional Misuse of NCIC

The incidents of unintentional misuse involved the use of NCIC by law enforcement agencies for noncriminal justice purposes. These purposes included conducting background searches on individuals applying for noncriminal justice employment such as shopping mall and school security guards, or on individuals applying for firearm permits, and liquor and taxi licenses. In addition to 6 of the 62 misuse examples we obtained, incidents of unintentional misuse occurred in 58 user agencies in 30 states and, according to some SCTA officials, may have resulted from misunderstanding the policy on use of NCIC for employment background investigations. The FBI has attempted to address the misuse problem by recommending training

and clarification of NCIC policies. Some agencies have attempted to implement such recommendations. For example, the South Carolina SCTA held a special training session for Alcohol and Beverage Commission agents who were requesting background searches for liquor license applicants and sent a letter to all NCIC users in the state reminding them of the proper uses of the system.

MOST INDIVIDUALS MISUSING NCIC WERE NOT CRIMINALLY PROSECUTED

The examples we obtained showed that most of the individuals misusing NCIC were not criminally prosecuted. Specifically, individuals in only seven of our misuse examples were criminally prosecuted. FBI and SCTA officials cited the lack of federal and state criminal statutes imposing penalties specifically for misusing NCIC as the reason prosecutors were reluctant to prosecute such incidents. For example, upon her discovery the terminal operator in the Pennsylvania incident was terminated from employment but was not prosecuted because of the lack of a specific statutory penalty for misusing NCIC. In another example, a dispatcher for a police department in Rhode Island conducted background searches on her fiance's political opponents. The dispatcher was terminated from employment but was not prosecuted because of the lack of an applicable statute.

Furthermore, even though some federal criminal statutes, such as theft of government property, computer fraud, and bribery have been used as the basis for NCIC misuse cases, such as those in Florida and New Jersey, FBI and SCTA officials and federal prosecutors regard these statutes as difficult to use in the prosecution of such misuse because they do not address NCIC specifically. For example, the local U.S. Attorney's Office investigating the misuse incident in Texas (discussed on page 16) declined to prosecute the police chief and the private investigator involved, citing the lack of a directly applicable federal statute. As part of a plea bargain, the investigator and the police chief each agreed to perform 160 hours of community service. The investigator had already been convicted for selling credit bureau information and had received a deferred sentence and a fine. In a letter to the FBI explaining his decision not to prosecute, the U.S. Attorney outlined the ineffectiveness of existing federal and state statutes in deterring NCIC misuse and called for a specific federal statute for such misuse. In response, the FBI's Legal Counsel Division pointed out that each of the existing statutes has technical defects that would discourage prosecutors, and indicated that it may be prudent to enact such legislation to protect NCIC from unauthorized access and use. The NCIC APB has also recommended enactment of federal legislation making NCIC misuse a specific federal crime.

When asked about solutions to the misuse problem, FBI officials in charge of NCIC and about half of the SCTA officials interviewed in our telephone survey expressed their support for federal legislation imposing penalties on those misusing NCIC. According to some SCTA officials, federal legislation would serve as a deterrent to potential misuse of NCIC. For example, according to a Pennsylvania SCTA official, if the terminal operator who helped her boyfriend had been arrested and prosecuted, her example could have served as a deterrent to others contemplating misusing NCIC. Federal legislation also would encourage prosecutors to prosecute individuals involved in such misuse. For example, according to a New York SCTA official, federal legislation would not only encourage U.S. Attorneys to prosecute misuse incidents but also would augment existing state statutes and serve as a strong deterrent to those contemplating misusing NCIC.

Currently, most user agencies and individuals who violate NCIC policies or misuse the system receive administrative sanctions. Specifically, local user agencies violating NCIC policy can have their access to the system temporarily revoked either by the FBI or SCTAs until the violations are corrected. The FBI has revoked the access of only one local user agency since NCIC became operational. SCTAs have also revoked the access of local user agencies to NCIC (see appendix II for examples). With regard to individuals who misuse NCIC, the NCIC Security Policy requires only that each criminal justice agency have appropriate written standards for discipline of such violators. Individuals who misuse NCIC have usually been either reprimanded by their agency, denied further access to the system, suspended without pay, or terminated from employment. Specifically, in 35 of our misuse examples, individuals were either reprimanded, terminated from employment, or received a variety of suspensions. There was no action taken in 7 examples, while the outcome was unknown or pending in 14 examples.

CONCLUSIONS AND RECOMMENDATIONS

We found that the NCIC system, being a network of coordinated state systems, is vulnerable to misuse because of various factors that increase its inherent risk and

because the controls of some state systems accessing NCIC are not adequate or are not being used effectively to deter and detect misuse. In an attempt to address NCIC's vulnerability, the FBI will implement new security measures for the Central Segment and its own workstations of the upgraded NCIC 2000 system. The implementation of NCIC 2000's security features is a positive development in the effort to address the system's vulnerability to misuse. However, the potential limitations and limited implementation of these features could diminish their effectiveness. Most significantly, the states will not be required to implement the security features. Consequently, the system will remain vulnerable to misuse.

Furthermore, SCTA officials identified certain barriers that may affect the overall implementation of NCIC 2000. First, funding shortages may prevent local user agencies from attaining the full potential of the new system and its security features. Second, hardware and software compatibility problems may affect timely implementation. Third, staff shortages at the FBI's Criminal Justice Information Systems Division will affect training and other technical assistance to the states. However, we believe that the NCIC user and contractor conference is a good forum to discuss and potentially resolve some of the capability and implementation issues we have identified.

We could not obtain assessments of the extent and nature of NCIC misuse because (1) the FBI and most SCTAs do not systematically maintain statistics or other information on misuse and (2) many state officials could not provide evidence to support their general assessments of misuse. However, we did obtain sufficient examples of misuse to indicate that such misuse occurred throughout the NCIC system and that misuse was both intentional and unintentional. Furthermore, all the reported misuse incidents involved insiders, while none involved outside hackers.

We believe that on the basis of our findings, misuse of NCIC is a problem that needs to be addressed more effectively. We emphasize that any measure aimed at making such misuse less likely can be effective only if implemented in a coordinated manner with other measures. For example, if NCIC 2000's security features are implemented and consequently detect more incidents of misuse, directly applicable legislation will be needed to ensure that the individuals responsible are prosecuted. On the other hand, while legislation will help prosecute some detected violators, without the additional security measures, some misuse may go undetected. We recommend that Congress enact legislation with strong criminal sanctions specifically directed at the misuse of NCIC. Such legislation should be aimed at (1) deterring individuals contemplating misusing NCIC and (2) facilitating and encouraging the prosecution of individuals who have misused NCIC.

In view of our findings and the NCIC 2000 implementation, we also recommend that the FBI Director and the NCIC APB re-evaluate the security specifications set forth in the NCIC Security Policy, particularly in the area of accountability. Recognizing the potential cost and implementation concerns involved, at a minimum, the FBI and the APB should amend the Security Policy to endorse and encourage state and local user agencies to enhance their security features, such as increasing user accountability through identification, authentication, and audit, to meet the C2 security rating.

AGENCY COMMENTS

Justice Department and FBI officials reviewed a draft of our testimony and agreed with our findings, conclusions, and recommendations. According to these officials, federal legislation will be very helpful in deterring insiders from misusing NCIC.

This concludes my prepared statement. In closing, I would like to acknowledge the cooperation of FBI and state and local law enforcement agency officials during the course of our review. I will be happy to answer any questions you may have.

APPENDIX I.—OBJECTIVES SCOPE AND METHODOLOGY

Our objectives were to (1) determine whether the FBI and user agencies have adequate controls to ensure that access to NCIC is for authorized purposes and deter and detect misuse of NCIC information and (2) obtain the FBI's and states' assessments of any NCIC misuse and examples of such misuse.

To fulfill the Subcommittee's request, we (1) interviewed FBI officials responsible for NCIC; (2) reviewed NCIC and state and local agency security policies and other relevant documentation; and (3) visited state and local law enforcement agencies who use NCIC in California, Nevada, and Texas and interviewed relevant agency officials.

We judgmentally[8] selected and visited the California Department of Justice and the Sacramento County Sheriff's Department, both in Sacramento, California; the Los Angeles County Sheriff's Department in Los Angeles, California; the Nevada Department of Motor Vehicles and Public Safety, and the Carson City Sheriff's Department, both in Carson City, Nevada; the Douglas County Sheriff's Department in Minden, Nevada; and the Texas Department of Public Safety, Austin Police Department, and Travis County Sheriff's Department, all in Austin, Texas. We did this work to obtain a description of the system and its controls and to learn how it operates. We also observed the physical security of NCIC terminals at the agencies we visited and the controls for accessing and disseminating information from the system.

In addition, we administered a telephone survey to all 54 SCTAs who oversee local user agencies in the United States and Canada to obtain information on (1) state and local agency access to NCIC, (2) access and dissemination controls, and (3) the extent of NCIC misuse and obtain examples of such misuse. We administered our survey between January 25 and February 18, 1993. While we did not verify the accuracy of the information provided, or its relevancy to NCIC, our survey instrument specifically solicited information about NCIC. During the interviews, we reiterated to the SCTA officials that our questions were specifically addressing NCIC.

It should be noted that the misuse examples we obtained were provided to us verbally and mostly without supporting evidence. Consequently, we could not verify the accuracy of these examples. Furthermore, the outcomes of five cases are still pending and the outcomes of eight cases are unknown. We characterized as intentional those examples which involved the use of NCIC for personal purposes, for profit, and for political gain. We characterized as unintentional those examples which involved the use of NCIC to conduct background investigations for noncriminal justice employment, or licensing purposes because of the apparent misinterpretation of policy prohibiting the use of NCIC for such purposes.

To obtain assessments of NCIC by computer security experts, we reviewed an NCIC risk analysis prepared by MITRE Corporation for the FBI in 1989; a report by Computer Professionals for Social Responsibility prepared for the Subcommittee on Civil and Constitutional Rights, House Judiciary Committee, in 1989; and a report by SRI International prepared for the FBI in 1990. We also interviewed the author of the SRI report.

To determine NCIC's inherent risk, we used the criteria contained in a GAO policy guide titled *Assessing Compliance With Applicable Laws and Regulations* (GAO/OP-4.1.2, Dec. 1989). This guide supplements the *Yellow Book* standards on internal controls.

We did our work between September 1992 and July 1993. We did not test the controls that are discussed in this report. Except as noted above, our work was conducted in accordance with generally accepted government auditing standards.

APPENDIX II.—EXAMPLES OF NCIC MISUSE

As part of our review of NCIC, we obtained 62 examples involving misuse of the system. Specifically, 33 of these examples involved the misuse of NCIC for personal purposes, 16 for profit, and 7 for political gain. Six examples involved the misuse of the system because of an apparent misunderstanding of NCIC policy.

We obtained the misuse examples from (1) the SCTAs we visited in California, Nevada, and Texas; (2) the nationwide telephone survey of SCTAs; and (3) the FBI, including its Office of Professional Responsibility. The examples we obtained are grouped by source. It should be noted that these examples were provided to us verbally and mostly without supporting evidence. Therefore, we could not verify the accuracy of these examples. Furthermore, the outcomes of five cases are still pending and the outcomes of eight cases are unknown.

SCTAs Visited

California

The California Department of Justice received a complaint from a person who suspected his employer of obtaining a copy of his criminal record from the NCIC's III file. A search of the state system's audit trail showed that the record had been accessed by a law enforcement agency in the eastern United States. Apparently, the employer had hired a private investigator, located in the eastern United States, to

[8] We used agency size and geographic location as the criteria for selecting our judgmental sample.

conduct background searches on prospective employees. The complainant's criminal history record was allegedly sold to the private investigator by an officer in a law enforcement agency. The employer then used the information to terminate the complainant from employment. As a result of an investigation, the private investigator and the officer disclosing the information will be prosecuted.

Nevada

A detective in the Las Vegas Metropolitan Police Department obtained NCIC information from an unsuspecting computer terminal operator, under the false pretense of legitimate police activity, and sold this information to a private investigator. The local U.S. Attorney declined to prosecute the case because of the lack of an applicable statute.

A tribal police agency on an Indian reservation accessed and released NCIC information to individuals connected to tribal elders. The SCTA revoked the agency's access to NCIC with no further action.

Texas

The city manager of a small town conducted NCIC inquiries on a political opponent using a terminal operator. The manager threatened the operator with loss of employment if she did not cooperate. The operator conducted the inquiries but also alerted the local police chief of her activities. In turn, the chief warned the manager about the unauthorized NCIC inquiries and fired the terminal operator for violating NCIC policy. In the meantime, the political opponent filed an official misconduct complaint against the manager, who was then arrested. In apparent retaliation, the manager fired the police chief before being arrested. The chief is considering legal action against the city to gain reinstatement. The city manager is being prosecuted under the state's official misconduct statute. However, the activities related to NCIC are not being prosecuted because of the lack of an applicable statute.

A computer terminal operator in a district attorney's office accessed and obtained NCIC information and disclosed it to her boyfriend. He, in turn, sold this information to private investigators. After an investigation, the operator was terminated from employment.

A sheriff and some of his deputies conducted NCIC inquiries on election challengers and found that one had been arrested for a weapons violation in 1968. This information was made public to discredit the challenger. A terminal operator who alerted the Texas Department of Public Safety of this misuse was fired by thesheriff. Other operators were threatened with similar action. A challenger won the election for sheriff, and no further action was taken.

A terminal operator in a sheriff's office accessed NCIC using fictitious identifiers and used the information he obtained for unauthorized purposes. An ensuing investigation could not conclusively determine the nature of these purposes. The operator received administrative sanctions.

Telephone Survey of SCTAs

Alabama

A law enforcement officer with authorized access to NCIC conducted employment background searches for a nationally known transportation firm in exchange for money. This incident was detected through the review of audit trail information. The officer was terminated from employment but was not prosecuted because the state attorney declined to prosecute the case.

Two law enforcement agencies conducted background searches using the III file for Alcoholic Beverage Control Board liquor license applicants. The outcome of this case is unknown.

A local sheriff's department conducted employment background searches on the III file for the state department of human resources. The outcome of this case is unknown.

Arizona

A former law enforcement officer used information obtained from three individuals in different law enforcement agencies to track down his estranged girlfriend and murder her. After an investigation, the printouts provided by the three individuals were discovered, and the individuals were identified, prosecuted, and convicted.

Arkansas

An ongoing investigation involves a terminal operator who allegedly sold NCIC information to an employer who wanted background information on a prospective employee. The case is pending.

Colorado

A private investigator paid several city employees to conduct NCIC record searches. During the service of a search warrant at the investigator's office in an unrelated fraud matter, state investigators discovered records indicating that payments had been made for NCIC records and notified the Colorado Bureau of Investigation. The ensuing inquiry, with the cooperation of the district attorney, resulted in the indictment of several individuals. Their state trials are pending. However, the local U.S. Attorney concluded that there was no violation of federal law in this case and declined to prosecute.

Connecticut

A state trooper provided a private investigator with information on individuals with NCIC records in exchange for money. The trooper was discovered by chance when the internal affairs department of the state police investigated the private investigator on an unrelated matter. The investigator maintained records listing the information provided, the dollar amounts involved, and his source (the state trooper). The state trooper was dismissed from employment.

Florida

About 2 years ago, a police chief's deputy accessed and obtained III file information and sold it to private investigators. The deputy has been indicted under Florida law for 100 counts of misuse. The case will be tried sometime this year.

A law enforcement agency conducted background investigations using the III file for taxi driver permits. The outcome of this case is unknown.

A police chief in a small rural town conducted background searches on prospective tenants in an apartment complex using the III file. The outcome of this case is unknown.

Iowa

Twelve cases of misuse have been reported to the SCTA during the past 2 years. These cases involved terminal operators conducting background searches on friends and relatives to determine if they had criminal records. None of these incidents involved the disclosure of information for money. The individuals involved received administrative sanctions.

Maine

A police officer conducted a background check on one of his wife's employees using the III file. The employee had a criminal record and was terminated from her position for not disclosing it. The officer conducted the check under the false pretense of a criminal investigation, with the full knowledge of his supervising sergeant. The terminated employee filed a complaint and the incident was investigated by the state police. After the investigation, the police officer and the sergeant were suspended for 2 days without pay.

A State Police officer disclosed the III file record of a drug dealer to this person. This incident was detected by an undercover agent, who was investigating a case involving the drug dealer. The state police requested that the FBI investigate the incident. However, since the incident did not involve money, the FBI declined to investigate. After a state investigation, the officer was demoted from major to lieutenant for misuse of NCIC.

Maryland

Several state police personnel checked the records of friends and relatives and provided information to these individuals about their records. The outcomes of these cases are unknown.

Several personnel from a local user agency checked the records of friends and relatives for these individuals. Some of the friends and relatives sold NCIC information to private investigators. The outcomes of these cases are unknown.

Montana

A law enforcement agency conducted criminal history searches on volunteers for the Big Brother, Big Sister program. These inquiries were technically violations of NCIC policy on background searches, but, according to a SCTA official, were apparently based on a misinterpretation of this policy. The case is still pending.

A law enforcement agency conducted criminal history searches on individuals residing in a privately owned and operated halfway house for the state corrections system. These searches were technically violations of NCIC policy, but, according to an SCTA official, were based on the lack of specific guidance to address such a unique situation. According to this official, the officers involved thought that they

were simply following their agreement with the corrections system. The case is still pending.

Nebraska

According to a SCTA official, numerous incidents involved criminal justice personnel who did not understand the proper use of NCIC and, thus, technically violated certain policies, particularly by conducting employment background searches. The outcomes of these cases are unknown.

New York

An insider from a law enforcement agency disclosed criminal history information to be used for employment background searches. A grand jury issued an indictment, but the insider was acquitted.

An insider from a law enforcement agency disclosed criminal history information to a local politician to be used against opponents during an election campaign. The insider received administrative sanctions.

North Carolina

A dispatcher accessed the criminal history record of her deceased husband seeking to erase it. However, her terminal was not authorized to erase the record. The dispatcher's activity was discovered during a state audit, and her operator certification was put on probation.

Ohio

An ongoing case may eventually involve law enforcement officials in other states and will be presented to a grand jury soon. The Ohio State Patrol received a "tip" that a detective used his position to obtain NCIC criminal history record information. He then sold this information to a private firm. This firm conducted employment background searches for Ohio-based companies. At least five other police officers in Ohio may be involved in this case; the detective is implicating his accomplices. In the meantime, the firm that hired the detective has moved to another state. Ohio is trying to prosecute this case under the Racketeer Influenced and Corrupt Organizations statute by charging the alleged criminals with grand theft of computer information.

Pennsylvania

A terminal operator in a user agency, involved in an election campaign, accessed and disclosed criminal history information on a political opponent. The operator was terminated from employment.

A police officer accessed and widely disseminated a fellow officer's criminal history record in order to discredit him. The officer was terminated from employment, settled a civil suit for $25,000, and was not prosecuted.

A computer terminal operator conducted background searches for her boyfriend, who was a drug dealer. He asked her to check the criminal history records of new clients to determine if they were undercover drug agents. Her activities were discovered when supervisors at the agency detected an unusual amount of inquiries from her terminal. Upon her discovery, the operator was terminated from employment but was not prosecuted because of the lack of an applicable statute.

Rhode Island

The weekly review of audit trail information discovered that a police department was conducting III file searches early in the morning using NCIC purpose code "J," which is used for criminal justice employment investigations. An investigation found that the unusual activity involved a dispatcher engaged to a local politician. This individual conducted background searches on her fiance's political opponents. The dispatcher was terminated from employment but was not prosecuted because of the lack of an applicable statute.

A state trooper conducted III file searches for his attorney who was defending the trooper against misconduct complaints filed by a private citizen. The trooper was investigated by a police panel of three peers and found "not guilty."

South Carolina

An employment firm obtained III file information from a law enforcement agency in Georgia. However, when this activity was discovered in Georgia, the firm began using an agency in South Carolina. This activity was also discovered, and the South Carolina SCTA revoked the agency's NCIC access.

A law enforcement agency conducted background searches on local politicians who were members of the city council. When a victim complained, this activity was discovered and administrative sanctions were imposed on those misusing the system.

The SCTA revoked the agency's NCIC access, and an individual was terminated from employment.

Tennessee

A mayor illegally fired the police chief and the city administrator of a small town and appointed a new chief. In a related action, the mayor ordered III file searches on the administrator in order to discredit him. The police chief and the administrator filed suit against the city and won reinstatement to their positions. The mayor's actions were voided, and her powers were curtailed by the city council. No further action was taken.

Virginia

During an election campaign, a sheriff released the criminal history record of an inmate in county jail. This inmate had written several letters to the local newspaper complaining about conditions at the jail and sought to embarrass the Sheriff during the campaign. In turn, the sheriff sought to downplay these charges and discredit the inmate, who already had an extensive criminal record, by releasing this information. The sheriff was charged with improperly releasing criminal history information under a Virginia statute. He was convicted on this misdemeanor charge and received a suspended sentence.

A state employee released criminal history information to a private investigator and was charged under the federal mail fraud statute. These charges were later dismissed because it was determined that the fraud statute was not appropriate for this case. The employee was terminated from employment. However, this individual filed a complaint with the state's grievance panel and won reinstatement through a binding ruling.

A chief of police released criminal history information to an unauthorized person. The state prosecutor reviewed the case and declined to prosecute. However, administrative sanctions were imposed on the chief whose access to NCIC was revoked for 60 days.

Washington

A police officer conducted criminal history searches from a court terminal and harassed a victim using this information. The officer used the court terminal instead of his own to disguise his identity. The outcome of this case is unknown.

A police officer disclosed criminal history information to a private investigator. This case is currently under investigation.

FBI AND FBI OFFICE OF PROFESSIONAL RESPONSIBILITY

A police chief of a small suburban police department provided criminal history information on individuals to a private investigator for nominal awards. The private investigator sold the information to nationally known firms, including a computer firm and a restaurant chain, which used the information to conduct preemployment background investigations. The FBI was alerted to the misuse by a disgruntled employee in the police department and investigated the case using audit trail information. On the basis of the investigation, a grand jury served subpoenas against the police chief and the private investigator. The investigator had already been convicted for selling credit bureau information and had received a deferred sentence and a fine. The assistant U.S. Attorney in charge of the case assessed the possibility of indicting the two individuals, but settled for a preindictment plea bargain, citing the lack of applicable federal statutes for misusing NCIC. Under a pretrial diversion program, the police chief and the private investigator agreed to perform 160 hours of community service.

An FBI special agent accessed and disclosed FBI records in NCIC for unauthorized purposes. The agent was censured, suspended for 10 days, and placed on probation.

A support employee disclosed NCIC information to an individual she was dating. The employee received a letter of censure.

A support employee disclosed information from NCIC's license plate file to an acquaintance. This person was being investigated by the FBI and was aware of the investigation, most likely through the information disclosed by the FBI employee. The support employee resigned from the FBI during the investigation and before the case could be referred for administrative adjudication.

A support employee disclosed NCIC information to a friend engaged in the repossession of automobiles. The employee advised the friend on whether the automobiles were stolen. The support employee resigned from the FBI before the case could be referred for administrative adjudication.

A support employee disclosed NCIC information to her father, who was serving a 10-year prison sentence for drug trafficking. An FBI investigation found that three additional persons received the NCIC information as a result of the employee's disclosures. The support employee was censured, suspended without pay for 14 days, and placed on probation for 1 year.

A support employee allegedly disclosed information from NCIC's III and driver's license files to a pawn shop, in exchange for interest-free loans. The employee denied any impropriety but resigned during the investigation and before the case could be referred for administrative adjudication.

An FBI special agent disclosed NCIC information related to a homicide case to a police department. An FBI investigation found that the agent was not acting in his official capacity when disclosing the information. The agent received a letter of censure.

A former FBI employee requested that a support employee provide NCIC information about the father of her child. The information was apparently needed to obtain public assistance. The support employee was orally reprimanded for providing the information.

Mr. CONDIT. Mr. Chairman, if you would like, I yield.

Mr. EDWARDS. Well, thank you.

That is an excellent statement.

I think we ought to make it clear that this information that is in the NCIC is public information. There is nothing, to my knowledge, secret in it; is that correct? And that is something that we have always insisted on, that it not include rumor, gossip, or investigatory information, and that is why we would not want—would not accept the inclusion of names of suspects of youth gangs or anything like that.

There is so much possibility for abuse. Every once in a while somebody wants to expand the system and include nonpublic information. And we have resisted that. What it generally has included is wanted criminals, stolen jewelry, stolen cars, missing persons.

I think there is only one instance where the NCIC is used we think inappropriately but for a good reason and that is the Secret Service uses it to track people that they deem possibly dangerous to a protected class of people such as the President, the Vice President, Mrs. Kennedy and President Ford, people like that. A few of them, I think around a hundred, are entered into the NCIC system. If they are stopped for a traffic violation or some other reason and the policeman in his patrol car asks the NCIC if this is a wanted person or any information about the person, that will instantly go to the Secret Service headquarters in Washington, and they will know that this person who might be dangerous is in a particular area where the policeman stopped the car.

We disapproved of that system, but they think it has some value. It is very limited and we are going to make sure that it is limited.

But I think, Mr. Chairman, that we would like some examples of the abuses. What kind of sales are made of this information?

This information has no business being peddled around and people making money out of it and it ought to be a crime. And it probably is some kind of a crime right now, theft of government property, but if your testimony is correct, it should be a much more specific and narrowly drawn statute.

Yes, this is public information, indictments and wanted persons and stolen property, that is public information, but we don't want people to take advantage of the FBI's collection, expensive and detailed collection of this, and it should be used strictly for law enforcement purposes.

Can some of you tell Mr. Condit and me more in detail, specific instances of the abuse of the system?

Ms. EKSTRAND. Mr. Bagdoyan will give some examples.

Mr. BAGDOYAN. Thank you, Mr. Chairman.

The first example is perhaps the most serious example of NCIC misuse that we encountered.

This incident occurred several years ago in Arizona where a former law enforcement official obtained NCIC and other information from a State system and also the department of motor vehicles, tracked down his ex-girlfriend, stalked her, and then eventually murdered her.

He obtained this information from three separate sources in local user agencies in his State. And the way these three individuals who provided the information were detected was through the discovery of printouts of the information in his apartment during the criminal investigation following the murder of his girlfriend.

The three individuals were charged with theft of computerized information. They were convicted, and I believe they still may be serving some time in State prison.

Of course, the individual who committed the murder has been convicted, also, and is serving life in prison for that crime. We also found several examples where——

Mr. EDWARDS. Let's go back to that instance.

Explain how the system itself was misused.

Mr. BAGDOYAN. The specific details, because of the passage of time, have been rather clouded. I think what happened was this individual asked specific information about relatives of his girlfriend, as this example was explained to me. And what happened, he used this information to track her down through her relatives and find out where she had moved to after leaving him. And eventually ended up stalking her, as I said before, not only her, but I believe her companion at the time, and eventually when she returned home from an outing, he was waiting for her and he proceeded to shoot and kill her.

Mr. EDWARDS. I have some difficulty seeing how the NCIC was involved in that, unless there was an arrest record or a conviction record or a wanted persons or something.

Mr. BAGDOYAN. I understand that. The way the example was explained to me by the gentleman who has the Arizona oversight agency, was that the information was used in combination with other sources, as I said the Arizona State system and also DMV records. Again, the specifics were kind of lost through the passage of time.

However, this gentleman did say that this example of misuse is used as a case study during NCIC training sessions to show what may happen to individuals who not only offer the information to outsiders who are not authorized to receive it, but also some of the, quote, unquote, "victims," some of them may end up being killed.

Mr. EDWARDS. The Arizona system might have a nonpublic information in it, like investigatory information.

Mr. BAGDOYAN. It is possible, yes.

Mr. EDWARDS. Or like another system, NLETS, has.

Mr. BAGDOYAN. That is correct.

Mr. EDWARDS. The police departments and FBI, they have to communicate investigatory information, you know, "We think there is a guy in Florida that you ought to look at, we have a report from an informant that he is so and so and doing this and that." Now that is very important for a criminal investigation, but that kind of information is not in the NCIC.

Mr. BAGDOYAN. That is correct. But it may very well be in the Arizona system. As I said before, this—it was used in combination from a variety of sources. I think this individual was very thorough in his search of his girlfriend.

As I said before, there were several other examples where insiders provided some information to private investigators, essentially sold this information to private investigators who in turn turned around and sold the same information to private firms in order to conduct background investigations on either current employees or potential applicants for employment with those firms.

Mr. CONDIT. What resources would be required to institute a level of management control that would be sufficient to identify or deter abuse? Can the FBI do more to improve oversight enforcement by the States?

Mr. BAGDOYAN. Within the context of NCIC 2000, it has been a major study undertaken since 1989. There are certain enhancements that are being offered in terms of access control software that will attain the C2 security rating, as Ms. Ekstrand described earlier. And essentially the security features are an attempt to make misuse less likely.

The contract for this system was awarded very recently and some of the technical details have yet to be worked out. There is a conference for that purpose upcoming sometime this fall, where you will have the user community, the FBI, and also the contractors involved in the contract getting together and hammering out the exact details from where the cost, the final cost, may be calculated.

I must say that we did request some contract cost information from the FBI, but this information was not provided to us.

Mr. CONDIT. Was there a reason why it wasn't provided?

Mr. BAGDOYAN. The reason essentially involved a statement to the effect that the contract involves still proprietary information and there was a reluctance because of that to provide that information.

Mr. CONDIT. There are lots of terminals and lots of people with access. Is it realistic to expect controls for improper use of the NCIC or is this a lost cause?

Ms. EKSTRAND. It is probably impossible to lock every hole. Considering that there are more than a million transactions a day, the number of abuses that we could find out about is really a very small number. It is just that the amount that can be tolerated for something like that is beyond minuscule, it has to be very, very, very small. It is probably a situation where you can never get to zero, but it seems clear that there are weaknesses in the system that can be improved to make it a lot less than it is now.

Mr. CONDIT. I take it that legislation with clear penalties would be helpful. But isn't preventing misuse principally a management problem and not a legislative problem?

Mr. HARRIS. I think it is a combination of both, Congressman. I mean it is partly management in that there are some things that could be done to tighten up the system and to monitor the system. And that is, in essence, the thrust of our recommendation, that they reevaluate the requirements.

But I think also the legislation, criminal statutes become a very important part of this, too, because I think even if you were to put every possible control in, you are still going to have situations where people will abuse the system. And so you need tight sanctions of some sort to prosecute those people, you know, time comes and you use that as a deterrent effect, hopefully prevent others from doing the same thing.

Mr. CONDIT. So you would suggest legislation to increase penalties for people who abuse the system?

Mr. HARRIS. Yes, some people, right.

Mr. CONDIT. I want to ask about the audit trails. How should audit trails be used to find misuse? Is there a preference in an audit trail, is there one that works, one that doesn't work?

Mr. BAGDOYAN. Different States maintain different types of audit trails. Essentially, an audit trail captures any type of information related to a transaction such as the terminal it originated from or the agency it originated from. Criminal history information inquiries require the entry of the original requester and the eventual customer, if you will, of that information.

The FBI maintains the master audit trail for the NCIC system for about 10 years. States are required to maintain criminal history information audit trails for a minimum of 1 year. And the other—the audit trail information for the other files in NCIC for a minimum of 6 months.

In terms of reviewing audit trail information, computer experts—computer security experts which we contacted, essentially believe in real-time audit of such information. It is an ongoing process rather than an occasional review if an incident arises or during the biennial audits that the FBI and the State control terminal agencies conduct of local users. We found several examples of a more thorough audit trail review process within an overall security-type arrangement.

One State, for example, has review of audit trail information on a monthly basis, in addition to surprise spotcheck visits to user agencies, in addition to the biennial audit. And they believe that is a pretty thorough program with which to not only detect misuse, but also to deter it. And that is just saying if you want to use NCIC for unauthorized purposes, we will be watching over you and you will be detected.

Mr. CONDIT. Your statement indicates that there are 1.2 million inquiries a day?

Mr. BAGDOYAN. That is correct.

Mr. CONDIT. If only one-tenth of 1 percent of the inquiries are abusive, that is still 1,200 a day and over 400,000 a year. What type of resources are needed to use the audit trail to find abuses in a large system? Do you have that defined?

Mr. BAGDOYAN. We weren't able to define that in terms of cost. Of course, the variety of agencies who would be reviewing the audit

trail information would have to deploy a certain number of resources. Whether they would hire additional people to do that or give the responsibility to supervisors, and so forth, we were not specifically looking at the cost implications of such audit trial reviews.

Mr. CONDIT. OK.

Mr. Chairman, I will yield back.

Mr. EDWARDS. The gentleman from North Carolina, Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman.

We addressed this problem, Mr. Chairman, about a year ago. I don't recall, Gary, whether you all were with us, whether we were in joint session or not. But at that time, I asked the panel to respond to us regarding the presence of State statutes in the various States. I realize that when prosecutors initiate criminal action, they probably are placed in a position of having to rely upon statutes which do not specifically address themselves to misuse of NCIC.

Would one of you all, for my benefit, give a brief overview of the laws that are currently on the books or available and which are used in the prosecution regarding misuse of NCIC, and the problems that these prosecutors may well encounter in having to rely upon these laws?

Mr. HARRIS. I think basically I—I am not a lawyer, Congressman. We have a lawyer with us. But I think the statutes that—I am not real familiar with all the State laws, but the statutes that have been used on the Federal, by the Federal Government, have been basically those dealing with theft of government property and computer fraud, and those types of laws, which weren't specific to NCIC.

Now, the States—and, Seto, I don't know if you picked up any of this in your conversations with the States—varies. And some of them, of course, don't have laws and others do. And those vary from State to State, for all 50 States.

Mr. BAGDOYAN. Mr. Coble, we found approximately, the exact number escapes me right now, that 28 States had some form of statute that may, in some cases, be used for NCIC. Based on my discussions with State officials, they emphasize that the use of these statutes essentially is at the discretion or the decision of a specific prosecutor. Some of these cases have been investigated and later declined because the prosecutor thought that it would be stretching the particular statute to apply to NCIC.

There have been instances where cases have been prosecuted for also accessing and obtaining information from the State system, rather than NCIC, and NCIC becomes just a part of that prosecution, although not specifically.

Mr. COBLE. Mr. Chairman, I imagine that the prosecutor very well may be placed in the position of having to force the pieces of the puzzle to fit very snugly. A statute may well be applicable in part, but not in toto, and then I can understand the frustrations that would follow.

Am I on the right course?

Ms. EKSTRAND. That is correct. I think it is perhaps some part of reluctance on the part of the prosecutor that because of the ambiguities that perhaps blocks some of the prosecutions, and that

means that people who violated the system are getting away with it to some extent.

Mr. COBLE. Thank you.

Thank you, Mr. Chairman.

Mr. CONDIT. Mr. Horn.

Mr. HORN. Thank you, Mr. Chairman.

I regret I am late for this hearing, but as the chairman knows, we all have other subcommittees meeting this hour.

Perhaps the question has been asked, but since we have this panel of experts in front of us, I am going to ask you one that comes up almost every day around here, not completely relevant, but maybe you can give us some insight. And that is the so-called instant check system, when it comes to the interest of one in securing a weapon.

Part of the problem has been the complexities of integrating 50 States' criminal information systems with any Federal system. And also the sheer cost of it. I wonder if you could give us some insight, based on your experience with this project, as to how long it would take to achieve a goal of a unified criminal data system, Federal and State, how much that might cost? And do we have any examples of any State where they have an instant check system now that truly is comprehensive in terms of their total criminal justice files?

Mr. HARRIS. I have to address that question generally, Congressman, because we haven't—I mean that mainly involves almost a complete study of its own. But I think generally we can say, based on the experience here and seeing how this system works and the fact that a lot of the States are doing different things, that it would be very difficult to develop such a system, not impossible necessarily, because of sovereignty and because of costs and those sorts of things.

And so when you talk about costs and you talk about time, I would just probably say a long time and a lot of cost. Because I think our testimony shows that there are a lot of situations where the States are doing things that are different, and the Federal Government has established for various reasons very minimum requirements to protect.

So based on our experience, not having looked, addressed your question specifically, it would be difficult.

Mr. HORN. I am assuming when we are talking about the data for such a system, we are talking about some of the basic things collected in the uniform crime reports, we are talking about also mental health incarcerations, temporary, what happened, et cetera?

Mr. HARRIS. Yes.

Mr. HORN. When you are talking about licensure for a weapon, you want to know has this person a mental health problem, have they a criminal record, so forth and so on. Is there any move in this area to get some uniformity of data input in the various States, just based on the categories in which the Federal Government might collect such information? And is there a need for some sort of Federal grant or State grant program to encourage that type of uniform data collection?

Mr. HARRIS. Well, again, I would address the gentlemen generally. I am not aware of any direct move to make things uniform. I think in the case of this study that we have done, certainly NCIC 2000 is a move in that direction, very definitely. And the extent to which that is adapted, you will have, you know, some uniformity. But everything is not going to be required.

Mr. HORN. So there would be basic similarity of data input from the State level and the Federal level in that system?

Mr. HARRIS. Seto, do you want to——

Mr. BAGDOYAN. Yes.

Essentially, Congressman, NCIC consists mostly of records from the State systems that are deposited in their own systems. And users throughout the country, whether they be Federal, State, or local agencies, can tap into that data base.

There are some FBI records in there, and as earlier someone else mentioned, there are Secret Service records in there for their protected list. In that context, I would like to comment further just a little bit.

Some of the examples of misuse of NCIC we found involved local user agencies using NCIC to determine if individuals should obtain firearms licenses or taxi permits or day care permits. NCIC policy currently forbids the use of the system for those purposes.

Mr. HORN. Why is that?

Mr. BAGDOYAN. It is essentially a policy definition that was established in, I believe, 28 CFR, section 20.33, which established NCIC as a centralized data base of shared systems. And it has been written in policy since that specific——

Mr. HORN. Well, I still ask, why is that? Because it is written in policy doesn't give me a reason. What is the reason for that approach?

Ms. EKSTRAND. I think the notion is——

Mr. HORN. I mean is it unreliable data, for example? That would be a reason for that approach.

Ms. EKSTRAND. I think the notion is that this is very sensitive data and it should only be used for the most important purposes.

Mr. HORN. I would say it is pretty important if you are purchasing a firearm.

Ms. EKSTRAND. It is probably an important purpose, but for the people that were establishing the system, the main purposes were for criminal justice employment or in relation to crime-fighting activities.

Mr. HORN. All of which I see relevant to the question I asked, and I can't understand why such data would be precluded from a law enforcement jurisdiction that wished to find out that, whether you are talking about recruiting law enforcement officers, whether you are talking about a potential criminal, or whatever. In other words, I don't understand the rationale, just because it is written in policy—which won't be the first time that disjunction has occurred.

Ms. EKSTRAND. Well, at the time the policies were established, concerns about firearms were probably not as great as they are today. So it is conceivable that time will change those policies.

Mr. HORN. Thank you, Mr. Chairman.

Mr. CONDIT. Thank you, Mr. Horn.

[Additional information concerning firearms purchaser screening follows:]

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

October 6, 1993

Honorable Don Edwards
Chairman
Subcommittee on Civil and
Constitutional Rights
United States House of Representatives
806 O'Neill House Office Building
Washington, D.C. 20515

Dear Chairman Edwards:

This is in response to your letter of July 28, 1993, in which you requested information concerning use of the National Crime Information Center (NCIC) Interstate Identification Index (III) for firearms purchaser screening.

Four states, Virginia, Delaware, Florida, and Wisconsin currently utilize III within a statewide, point-of-sale firearms purchaser screening program. California and Maryland utilize III in statewide programs based on processing of applications during a waiting period.

Firearms licensing and permit screening by a criminal justice agency, because of its vital effect on the prevention and detection of crime, is regarded as a criminal justice purpose when required by a Federal, state, or local law. A number of state and local criminal justice agencies use III for such purposes. It is difficult to ascertain the extent of such use at this time because the purpose designator used for such requests was previously purpose code "C" which is used for all criminal justice purposes. Purpose code "F" was only recently created for firearms screening use. Our records for the month of August, 1993, show that purpose code "F" transactions originated in 34 states, though of these, only eleven had a significant (over 1,000) number of transactions under this purpose code. The total number of III inquiries in August, 1993; under purpose code "F" was 125,126.

Your request for the information provided above arose from testimony to your Subcommittee by the General Accounting Office (GAO) on July 28, 1993, concerning misuse of NCIC/III information. I would like to take this opportunity to note that we take issue with both general conclusions and specific factual

matters contained in that testimony. Though we support GAO's conclusion that Federal legislation is needed to deter NCIC misuse, we believe that testimony exaggerated the magnitude of NCIC/III misuse and misstated specific factual matters.

Prior to testifying, GAO staff met with FBI Audit Section Staff and Department of Justice (DOJ) Computer and Telecommunications Staff (CTSS) to provide an opportunity for comment. The testimony indicated that the FBI and DOJ CTSS were in agreement with GAO's "findings, conclusions, and recommendations." That representation is misleading. Substantive disagreements and corrections were discussed which would have improved the accuracy of the testimony and placed its finding and recommendations in proper context. DOJ's CTSS, among other written comments, stated to GAO that "given the volume of transactions the NCIC transmits and receives daily, the reported alleged incidents may represent a relatively small occurrence rate of misuse. Therefore, the probability of occurrence for this threat may be significantly lower than is intimated in this report." This comment is consistent with verbal comments also made by FBI Staff to GAO representatives prior to your hearing. The volume of transactions against which the three-year total of 62 misuse incidents should be measured is approximately 1.2 billion transactions in the same three years.

GAO also intimated in its testimony that NCIC misuse may be undetected, and when detected, is often unpunished. In actual fact, every example of misuse identified by GAO was provided to GAO by the FBI or an NCIC Control Terminal Agency (CTA). There is no support for any inference that misuse is undetected. The absence of criminal prosecutions in many misuse incidents is not indicative of a lack of punishment or a lack of aggression by the FBI or CTA's in pursuing sanctions. GAO acknowledged at one point that the misusers "have generally received administrative sanctions." Virtually every misuse cited by GAO resulted in some sanction being applied. Though the FBI strongly supports strengthening the capability for effective criminal prosecutions, an administrative sanction can often be more appropriate to the offense.

GAO personnel, in subsequent contacts with the FBI, have acknowledged misstatements as to the two most egregious examples of misuse contained in the testimony. GAO has indicated that the testimony will be corrected. These inaccuracies contributed to the exaggeration of the magnitude of the misuse problem. Written correspondence has been directed to GAO concerning both these specific factual inaccuracies and general conclusory issues.

The FBI continues to support the GAO recommendation for legislation. The nature of the System and security controls in effect are such that "insider" misuse is the primary, if not the only, recognized risk. Though the user community is highly "trusted" because of extensive and mandatory background screening, criminal penalties would be useful in deterring such misuse as exists. As you know, the FBI sought NCIC-related legislation long before the GAO study and testimony.

I trust that I have responded adequately to your inquiry.

Sincerely yours,

David F. Nemecek
Inspector-Deputy
Assistant Director
Criminal Justice Information
Services Division

Mr. CONDIT. Ms. Woolsey.

Ms. WOOLSEY. Thank you, Mr. Chairman, and thank you for the coffee. I have never been treated so well at a hearing.

Mr. CONDIT. I try to take care of you.

Ms. WOOLSEY. I will make sure I get here on time next time.

I am sorry I am late, I am sorry I missed your testimony. And I have a question of each of you, if you think you want to answer it, but you may have already. But just for my own help, what are your major recommendations to prevent insider abuses and to—what are you recommending that we do to improve practices and policies so that we can feel more secure about this?

Ms. EKSTRAND. I think we at least have to get to the C2 level of security in relation to this entire system, which means individual identification, authentication, and audit, to protect the system as a whole.

Ms. WOOLSEY. Passwords and——

Ms. EKSTRAND. This is individual passwords, some type of authentication such as fingerprint analysis to ensure that it is the right person. And then audit to determine—to keep monitoring whether there has been inappropriate use or not. But this is a very expensive proposition and at this point is something that each State and local government, all of the users all the way through the system would have to be willing to spend the money to do. And that is probably a very hard thing to do.

Ms. WOOLSEY. And have you looked at the cost-benefit of a program like that?

Ms. EKSTRAND. It is very, very difficult to do any kind of cost-benefit analysis in this situation. The benefits of not having misuse of the system is something that is very, very difficult to quantify.

Ms. WOOLSEY. Any of the others, do you have——

Mr. BAGDOYAN. I think the other recommendation we are making essentially is to enact legislation that would at least act as a deterrent to individuals who may contemplate misusing the system. And this goes essentially hand in hand, that you need a combination of different measures in order to make misuse less likely.

As we have mentioned earlier, you will probably not eliminate this activity entirely, but you can certainly be able to make it less likely through a combination of different measures, whether they be legislation or specific security measures.

Ms. WOOLSEY. Well, who should be the lead agency to make this happen, the States or the FBI? Who is primarily responsible?

Mr. BAGDOYAN. The way the NCIC system is currently set up, there is the Advisory Policy Board which is made up of 20 elected members from the user community and 6 appointed members from the criminal justice community, who advise the Director of the FBI on policy and other issues that affect NCIC. The FBI is essentially responsible for management of the overall system, and the next level below them are the State control terminal agencies which oversee local users at the State level. And then the local agencies will be the bottom of that rung, essentially, that they run their own small systems on a daily basis.

The way NCIC is set up, you would essentially need a coordinated way of dealing with every and each issue.

Ms. WOOLSEY. But you need us to say that we want the FBI to start the process, or could it start at the State level? Somebody has to lead this. I mean we can't just throw it out there and say fix it.

Mr. BAGDOYAN. The recommendation we are making in terms of reevaluating the current security requirements and policies for NCIC, is directed at the Director of the FBI and the Advisory Policy Board, who are essentially the leaders of this system. In that respect, I would imagine it would be up to them to coordinate their efforts on down the way, the ladder, so to speak, that I described earlier.

Ms. WOOLSEY. Well, I hope to know more about this as I am around here longer, so I can be more helpful.

Mr. Harris.

Mr. HARRIS. I was just going to add, I think that leadership in this area needs to come from the FBI, but they need, of course, to work very closely with the NCIC Advisory Policy Board. And I think that is the whole essence of our second recommendation, which what we are really saying is, look, NCIC 2000 effort is a good step forward in the direction of tightening up things, but there are some problems with it, implementation. And what we are recommending is that the FBI and the Advisory Board reevaluate, based on NCIC, what are their current requirements, and revisit those. And are there some requirements that could be increased?

And I think in that area, we are most concerned with individual identification, authentication, and accountability. But I think the other part of our recommendation is important because the second part of it says that, look, we recognize that there are going to be situations where certain entities, units out there using the system, are not going to have the money to do some of these things. And so as a policy board, you need to at least identify those things which would be really good options. If you had the money to pay for them, they would tighten up the system. And as a national policy recognize this and encourage the States to, in addition to the requirements, to adapt these other things voluntarily.

Mr. CONDIT. Mr. Hyde.

Mr. HYDE. Thank you, Mr. Chairman.

I have no questions, other than to express my appreciation for the work done by the GAO and reaffirm what Mr. Edwards said, that our subcommittee will be looking at legislation. He hopes to have a markup in the fall. It seems to be very much needed.

Thank you.

Mr. CONDIT. Thank you.

[The prepared statement of Mr. Hyde follows:]

PREPARED STATEMENT OF HON. HENRY J. HYDE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

The National Crime Information Center provides accurate, verified information on wanted persons, stolen property and criminal history records. It is an extremely valuable resource, and as such, is subject to improper or unauthorized use. At the request of Mr. Condit, Chairman of the Subcommittee on Information, Justice, Transportation, and Agriculture, the General Accounting Office has performed a review of NCIC to determine if the system has adequate controls to prevent misuse the nature and extent of such misuse.

The GAO report shows that the main threat to the integrity and security of the NCIC system comes from the inside—the authorized user who improperly obtains

information for personal or financial gain. As our witnesses will testify today, there are no state or federal statutes which specifically address this problem.

Mr. CONDIT. Mr. Nadler.

Mr. NADLER. Thank you, Mr. Chairman.

Ms. Ekstrand, in your statement you say that in addition to the NCIC being inherently risky, many State systems lack appropriate controls for accessing NCIC because they lack individual user identification, authentication, accountability, and various other problems. And you also state that because the NCIC is a network of coordinated State systems and the information can be accessed from any system, the control limitations in any one system render the entire network vulnerable to misuse. In view of this, if we are going to protect the system from misuse and protect people's privacy rights, do you think that we are going to have to mandate some limitations on the States, we are going to have to mandate that they have adequate systems to protect access to NCIC, as condition of accessing NCIC for that State?

Ms. EKSTRAND. It is a difficult situation. I mean, there is great importance to having this system from law enforcement standpoint. And we certainly don't want to expel States because they are not meeting certain standards. And there is certainly also a question of State sovereignty that has to be considered.

Mr. NADLER. Let's put it this way, the conclusion that one comes to from reading your statement is that no matter what we do here in Washington from the Federal angle, if we don't mandate certain minimum levels of control on State access, then the system is still going to be very vulnerable.

In other words, you can't protect it only from the Federal access side; is that correct?

Ms. EKSTRAND. You can't protect only from the Federal standpoint, that is correct. Each State system would have to get to that C2 level of security to at least meet that minimum level.

Mr. NADLER. Now what would you estimate the odds of all the State systems getting to the C2 level of security without some sort of mandate from Washington are?

Ms. EKSTRAND. Financially, it would be very, very difficult for the States, all of the States to do this. I think the target date is 1998, to have the States voluntarily to get to that level. It would be very unlikely that that will happen.

Mr. NADLER. It is unlikely they will meet the target date of 1998?

Ms. EKSTRAND. I think it is unlikely because of the costs involved of doing that.

Mr. NADLER. So in other words, if we are going to have a safe system, safe from abuse, in addition to whatever we do on the Federal level, we would have to in some way even mandate or pay for or somehow get the States to go there, too, because it is not going to happen in the normal course of events?

Ms. EKSTRAND. Well, there is always a balancing act as to what you want to spend your money on.

Mr. NADLER. We understand that. But is it correct or not that in your estimation unless we either pay for the States doing this or mandate that they do it without our paying for it, but in some

way act on the States, that it is unlikely that they will get to the C2 level of security that will have a safe system?

Ms. EKSTRAND. It seems very unlikely that all States would be able to get to that level, for a large part because of financial reasons.

Mr. NADLER. And any one State not getting to that level, renders the system subject to this kind of abuse?

Ms. EKSTRAND. It could render the system subject to abuse. It provides the, you know, the weak link in the chain, where someone who wanted to abuse the system could enter the system.

Mr. NADLER. In other words, it is safe to say that this is a problem that we have to address if we want a safe system, the State problem is a problem we have to address?

Ms. EKSTRAND. That is correct.

Mr. NADLER. Thank you.

Ms. WOOLSEY [presiding]. I have one more question. It has to do with the simplest method, which sometimes is the most effective. Is there anything such as a message on the screen for legitimate users, that warns them about the illegality of passing on information or anything like that?

Mr. BAGDOYAN. Yes, Ms. Woolsey. Several of the local user agencies that I visited had certain demonstrations of how to access the system. And on occasion on the screen, there are top and bottom messages that either flash or are in bold print, warning the user that this is for authorized criminal justice purposes only. And that is about the extent of it.

There are, of course, training manuals and training sessions that purportedly highlight the use of the system for authorized purposes only.

Ms. WOOLSEY. But it is not totally consistent? It is not on every screen?

Mr. BAGDOYAN. Again, yes, it reflects the diversity of having 19,000 different systems that access NCIC directly and then you have another 51,000 who access it indirectly. It is quite a collection of different systems.

Ms. WOOLSEY. Well, does anybody else—everybody left. Does anybody else have anything else?

All right.

Thank you so much for coming and sharing your information with us.

And the hearing is adjourned.

[Whereupon, at 10:54 a.m., the subcommittees adjourned, to reconvene subject to the call of the Chairs.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

September 29, 1993

Ms. Laurie E. Ekstrand
Associate Director
Administration of Justice Issues
General Government Division
Washington, D.C.

Dear Ms. Ekstrand:

On July 28, 1993, you testified before a joint hearing of the House Subcommittee on Information Justice, Agriculture and Transportation, Committee on Government Operations and the House Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary. Your testimony was entitled "Legislation Needed to Deter Misuse of Criminal Justice Information," but was essentially directed at a review conducted by GAO of informational security within the National Crime Information Center (NCIC) System. The FBI strongly agrees with your primary recommendation that Congress enact specific legislation which would effectively penalize misuse of NCIC. In fact, though not revealed in your report, the FBI and the NCIC Advisory Board had recommended such legislation well before GAO's study was conducted. In spite of our agreement on the need for legislation, we believe your report to be inaccurate generally in its findings and conclusions, and in several specific instances to be factually inaccurate.

The FBI was afforded the opportunity to discuss a draft of your testimony with several GAO investigators, including Mr. Bagdoyen, on July 23, 1993. We offered several comments that we believed then, and still believe, would have improved the accuracy of your testimony. Despite assurances that the substance of these comments would be included, your testimony indicated only that the FBI and the Department of Justice (DOJ) "agreed with our findings, conclusions, and recommendations." Though we acknowledged agreement with one of your recommendations, this was a gross mischaracterization of our comments and was extremely misleading. Our previous comments and those of the DOJ Computer and Telecommunications Security Staff, had they been included in your testimony, would have provided a properly balanced context for your recommendations.

One of the contextual issues discussed with the GAO Staff was the extent that misuses are unpunished and/or undetected. We noted that every one of the incidents revealed in your testimony had been previously provided to GAO by the FBI or NCIC Control Terminal Agencies. Further, virtually everyone of these incidents had resulted in some disciplinary action up to and including criminal penalties. These facts tend to belie the suggestion implicit in your testimony that misuse is largely unknown and largely goes unpunished. In fact, as we pointed out to your investigators, disciplinary action appropriately varies with the severity of the offense. Termination of employment with a criminal justice agency can be a severe penalty. This point was not corrected or even discussed in your testimony.

We also discussed the size and nature of NCIC, which we believe to be highly relevant to your testimony. Comparison of the 62 incidents of misuse identified in your testimony to the approximately 1.2 billion NCIC transactions processed in the same three year period negates any implication of widespread abuse. Again this context was not provided in your testimony.

We believe that a clear understanding of NCIC and its uses is necessary to understanding NCIC security requirements. NCIC is designed to be available, within seconds, to every police officer in the United States. Security is designed with this paramount goal in mind. Hence, great reliance is placed on secure locations which are accessible only by criminal justice personnel carefully screened in advance. Security measures, such as end-to-end encryption, would have minimal benefit to a system which does not have a significant outsider intrusion problem. Your testimony fails to distinguish those NCIC 2000 security measures properly applicable at all levels from those needed only for a portion of the system.

Specific examples of factual inaccuracy can be found in to your testimony. Your testimony identified a case in Arizona where a former law enforcement officer located and subsequently murdered his former girlfriend. Computerized system printouts provided by active law enforcement officers were used to locate the victim. This example was offered in the context of "NCIC misuse," but relevant information as to the victim's location came only from Department of Motor Vehicle (DMV) systems. No information of any kind was obtained by the perpetrator from NCIC. An NCIC Wanted Person File inquiry was made only because it is automatically requested by the local system when a DMV check is made. The NCIC response was, in fact, a "no record" response.

Also in your testimony, you identified a case in Texas involving misuse of NCIC information by a local police chief. We were surprised by this allegation and subsequent to your testimony attempted to discover more details of this incident. We were unable to identify any incident in Texas involving a chief of police or official of such stature. Further review by Texas agencies with Mr. Bagdoyen of GAO's Los Angeles office reveals that the case identified in your testimony was inaccurately reported and no such incident occurred. These factual inaccuracies exaggerated the seriousness of misuse incidents and, as such, were misleading as to the seriousness of the misuse problem.

The FBI and the NCIC Advisory Policy Board believe that security policy and enforcement appropriate to the sensitivity of the information in the System should be reviewed frequently. We also believe that the features present in NCIC 2000 will appropriately enhance system security. NCIC security policy will continue to undergo significant review and improvement in the future. Though we may disagree with your testimony, it is our hope that it will contribute to achieving legislative action to provide criminal penalties to deter insider misuse.

As always, my staff is available to discuss these matters with you.

Sincerely yours,

Udy C. Wood
Acting Chief
Audit Section
Criminal Justice Information
Services Division

U.S. Department of Justice

Washington, D.C. 20530

DEC 21 1993

Honorable John Glenn
Chairman
Committee on Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Pursuant to the requirements of 31 U.S.C. §720, the Department of Justice is responding to the General Accounting Office (GAO) recommendations contained in its testimony, entitled "National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information." Although the Department accepts, in principle, the GAO assessment of the security posture of the current National Crime Information Center (NCIC) environment, we believe that, in failing to put its findings in a proper context, GAO misleads its audience as to the frequency of abuse and the aggressiveness of system participants in detecting and punishing misuse.

Any large, distributed, heterogeneous, computing environment that has a geographically dispersed user base with multi-jurisdictional and functional requirements and that also produces large volumes of transactions has an inherent vulnerability from authorized users. One important aspect of the NCIC environment, however, that significantly reduces this inherent vulnerability, is that the user community consists of individuals who are in positions of trust. Further, even though the testimony cites several possible incidents of misuse, it is important to note that given the volume of transactions the NCIC transmits and receives daily, the reported alleged incidents represent a relatively small occurrence rate of possible misuse. Therefore, the probability of occurrence for this threat may be significantly lower than is intimated in this testimony. Nonetheless, the Department believes that implementation of the GAO recommendations can improve the NCIC program.

GAO recommended that the Director, Federal Bureau of Investigation (FBI) and the NCIC Advisory Policy Board re-evaluate the security specifications set forth in the NCIC Security Policy, particularly in the area of accountability. At a minimum, GAO suggested that the Security Policy be amended to endorse and encourage State and local user agencies to enhance their security features.

All NCIC policy is subject to continuous review by user agencies, representative Regional Working Groups and the NCIC Advisory Policy Board. The NCIC Security Policy was developed and refined through this review process. It explicitly states that stricter measures can be adopted by the States.

More rigorous technical and procedural controls already planned will further enhance the security of NCIC resources. Proper implementation of the security features of NCIC 2000 will significantly improve the level of security over the current system. However, the FBI has recognized that State and local funding may not be available to allow broad implementation of all NCIC 2000 security features at all levels. It is the goal of the FBI and NCIC Advisory Policy Board to improve security as resources permit.

GAO also recommended that Congress enact legislation with strong criminal sanctions specifically directed at misuse of NCIC. The Department agrees that statutory penalties for unauthorized use of the NCIC system by authorized personnel would provide a significant deterrent to such activities. The FBI will continue its efforts to seek enactment of NCIC-specific legislation as the best means of deterring abuse of the system by authorized users.

Should you have any questions concerning this response, please feel free to contact me.

Sincerely,

Stephen R. Colgate
Assistant Attorney General
for Administration

cc: The Honorable Gary A. Condit
Chairman
Subcommittee on Information, Justice,
Transportation and Agriculture
Committee on Government Operations
U.S. Representatives

The Honorable Don Edwards
Chairman
Subcommittee on Civil and
Constitutional Rights
Committee on the Judiciary
U.S. House of Representatives

The Honorable Charles A. Bowsher
Comptroller General of the United States

The Honorable Leon E. Panetta
Director, Office of Management and Budget

Henry Wray
Director
Administration of Justice Issues
General Government Division
General Accounting Office

BOSTON PUBLIC LIBRARY
3 9999 05983 030 5

ISBN 0-16-046181-2